ANÁLISIS DE AMENAZAS Y VULNERABILIDADES

Modelo SOCIA. Una reflexión conceptual y práctica desde la perspectiva del adversario

Jeimy J. Cano M.

Resumen— El objetivo de este artículo es presentar una propuesta metodológica denominada SOCIA para modelar al adversario y sus movimientos inesperados a partir de la incertidumbre, que incluyendo las reflexiones de los diferentes actores organizacionales, permite elaborar una visión diferente y complementaria para comprender mejor los retos y acciones de los atacantes. Para ello, se aplicó el instrumento desarrollado por cada uno de los elementos que constituyen la propuesta en el departamento de auditoría de una institución financiera, que organizado en grupos de trabajo interdisciplinarios, procedió a analizar varios casos de ciberataques en el sector bancario. Los resultados del ejercicio permiten construir una visión más elaborada y enriquecida de los riesgos actuales desde diferentes perspectivas para realizar simulaciones que desafían los mecanismos de seguridad y control actuales, y así poner de manifiesto posibles puntos ciegos en sus procesos y en la infraestructura tecnológica actual. En consecuencia, la SOCIA, crea un lenguaje común para elaborar una comprensión de la dinámica del adversario, no sólo a partir de su capacidad técnica, sino de sus técnicas y estrategias para configurar la acción no autorizada, aumentando la conciencia de la empresa sobre las capacidades del agresor y su impacto en la promesa de valor de la empresa.

Palabras clave — Adversario, Amenazas emergentes, Consciencia situacional, Estándares, Confianza

I. INTRODUCCIÓN

CON el pasar del tiempo, las prácticas de seguridad de la información han venido evolucionando tratando de establecer una nueva frontera de protección, que demore al atacante y trate de disuadirlo de sus acciones contrarias frente a los activos de información estratégicos de las organizaciones. En este ejercicio, se han actualizado las normas ISO, los marcos de trabajo disponibles en tecnología de información, así como los listados de controles que las empresas desarrollan para establecer su línea base de operaciones y sobre la cual, cada cierto tiempo se adelanta su validación de efectividad por parte de las áreas de auditoría de tecnología de información [1].

Si bien estas actividades, se han convertido en “*commodities*” de la práctica de seguridad de la información, el atacante no ha caído en esa realidad y por el contrario, ha avanzado en su capacidad de afectación y agresión, en niveles más sofisticados, menos visibles y más efectivos, adoptando las nuevas posibilidades tecnológicas y explorado nuevas vulnerabilidades del entorno [24], fruto de la mayor densidad digital disponible ahora en un escenario más hiperconectado y tecnológicamente modificado [2, 19].

En consecuencia, contar con prácticas estándares de seguridad de la información, si bien permite a las organizaciones asegurar un espacio de acción frente a las amenazas conocidas, deja poco margen para que puedan responder o anticipar, las propuestas inciertas de los agresores, que por lo general terminan sorprendiendo tanto a los especialistas en seguridad de la información, como a las diferentes áreas de las empresas [3, 25]. Lo anterior revela las limitaciones inherentes de los estándares conocidos, que implica una revisión en detalle de los nuevos entornos de operación de las empresas, mediados por redes sociales [30], para repensar nuevamente dichas prácticas y pensar ahora, en el desarrollo de capacidades distintivas para atender los retos de la protección de la información.

Dicho lo anterior, se hace necesario reflexionar sobre la manera de incluir la figura del adversario en los marcos de seguridad y control disponibles a la fecha, considerando que éste y sus técnicas son el nuevo reto a comprender, atender y superar, de tal forma, que no sólo sea la vista del analista tradicional de seguridad de la información, basado en un listado de controles el que atienda las realidades emergentes del contexto organizacional [26], sino que éste desarrolle una capacidad de análisis, prospectiva y aprendizaje que le permita caminar en terrenos algunas veces inciertos y en otros, inesperados, para tratar de descifrar las estrategias de los atacantes y así, proponer acciones alternativas de mitigación o contención, teniendo presente que en algún momento el agresor va a tener éxito [4].

De acuerdo con lo expresado previamente, este artículo presenta una propuesta conceptual y práctica para modelar el adversario. Su diseño busca complementar los análisis ya existentes de los entornos de las organizaciones, para que apalancados en una visión sistémica de riesgos (conocidos, latentes, focales y emergentes) [5], se puedan plantear escenarios de análisis prospectivos, basados en casos previamente documentados, experiencias propias de la industria o alternativas novedosas que los propios analistas de seguridad de la información u otros perfiles que puedan sugerir, con lo cual se habilita a la organización para anticipar amenazas emergentes que posiblemente no se hayan identificado previamente.

Por tanto, este documento para dar cuenta de sus reflexiones se organiza de la siguiente manera: en la sección II se presenta una revisión y análisis de algunas propuestas actuales sobre el modelaje de amenazas; en la sección III se introduce el

modelo SOCIA como una propuesta conceptual que sugiere una vista ágil e inclusiva del adversario. En la sección IV se presenta y explica el uso del modelo en un caso particular utilizado en un taller en una entidad financiera, y finalmente en la sección V se plantean algunas conclusiones sobre el modelo presentado y su aplicación.

II. MODELANDO LAS AMENAZAS. REVISIÓN DE ALGUNAS PROPUESTAS VIGENTES

Entender al adversario no es un tema nuevo en seguridad de la información. Es una dinámica que en muchas ocasiones se usa para tratar de advertir alguna violación de un control o acción adversa de un individuo frente a la protección de un activo. En este sentido, los profesionales de seguridad de la información encuentran en la forma de pensar del atacante, una vista de aquello que puede salir distinto a lo planeado, y poder ver cómo es posible superar o afectar la medida de protección previamente instalada y probada en el sistema o activo protegido [23].

Sin perjuicio de lo anterior, y considerando la inestabilidad del entorno de operaciones actual de las organizaciones, se han venido desarrollando propuestas alternativas que buscan modelar las actividades y tácticas de los atacantes, tratando de establecer algunos parámetros de análisis detallados, generalmente basados en ataques previos documentados, con el fin de establecer un perfil del agresor que pueda ser visualizado desde las estrategias utilizadas y las acciones técnicas realizadas, para configurar una “firma” del adversario que ilustre a los analistas cómo es su modo de operación y así advertir, las acciones de mitigación o contención necesarias de forma anticipada [6].

Dentro del listado de propuestas de modelaje de amenazas se encuentran las siguientes: [22]

- STRIDE – Inventado por Loren Kohnfelder y Praerit Garg en 1999 y adoptado por Microsoft en 2002. Ha evolucionado con el tiempo incluyendo las variantes STRIDE por elemento y STRIDE por interacción.

- P.A.S.T.A (*Process for Attack Simulation and Threat Analysis*) - es un marco de modelado de amenazas centrado en el riesgo desarrollado en 2012 por Tony Uceda Vélez. Contiene siete etapas, cada una con múltiples actividades.

- *Attack Trees* - Desarrollado por Bruce Schneider en 1999, se aplicó inicialmente como método propio. A la fecha se ha combinado con otros métodos y marcos.

- *CyberKill Chain* – Desarrollado por la firma Lockheed Martin en 2011. Es una metodología aceptada por la industria para entender cómo un atacante llevará a cabo las actividades necesarias para causar daño a una organización.

- MITRE ATT&CK (Tácticas, Técnicas y Conocimiento Común de Adversarios) – Desarrollado por el MITRE² en

2013. Es una base de conocimientos de acceso global sobre tácticas y técnicas adversarias basadas en observaciones del mundo real.

A continuación, se detallan cada una de ellas.

A. STRIDE

STRIDE, es el acrónimo de seis amenazas claves (en inglés) que establece este método para modelar las posibles acciones de los adversarios: *spoofing*, *tampering*, *repudiation*, *information disclosure*, *denial of service* y *elevation of privilege*, que traducido al español se leería como suplantar, alterar, repudiar, revelar información, denegar el servicio, y elevar privilegios. Esta propuesta puede ser utilizada desde múltiples enfoques: como una forma para pensar como el atacante y establecer maneras de vulnerar el sistema; como una forma de analizar los elementos del sistema y sus vulnerabilidades o como una estrategia para atacar las interacciones que tiene el objeto bajo evaluación con sus otros componentes [7].

Con este método, los analistas o personas participantes de la revisión del sistema bajo evaluación procuran establecer aquellas cosas que pueden salir mal con el sistema, los momentos o acciones que se pueden materializar y afectar el adecuado funcionamiento del mismo. De igual forma, por cada amenaza enumerada se tiene el principio y/o servicio de seguridad que se requiere asegurar indicado entre paréntesis: *spoofing* (autenticación), *tampering* (integridad), *repudiation* (no repudio), *information disclosure* (confidencialidad), *denial of service* (disponibilidad) y *elevation of privilege* (autorización) [6].

Adelantar un ejercicio siguiendo lo sugerido por STRIDE, permite tener un escenario base de amenazas en los diferentes puntos del sistema objetivo, los cuales son insumo para entender los impactos de su malfuncionamiento, uso inadecuado o falla, así como para plantear los mecanismos de seguridad y control requeridos para hacerlo más resistente a los ataques. El método prevé algunos controles para cada uno de los principios y servicios de seguridad asociados con las amenazas.

B. P.A.S.T.A

El proceso de simulación de ataques y análisis de amenazas establece siete (7) pasos metodológicos claves para establecer el marco de acción frente a situaciones inciertas del sistema o componente que se analiza: [8]

- *Definir los objetivos* – Este primer paso incluye detallar los objetivos de negocio que desarrolla el sistema, enumerar los requerimientos de seguridad y cumplimiento necesarios y el análisis de impacto en el negocio si este componente o pieza de software falla.

- *Definir el alcance técnico* – Esta fase demanda establecer los límites técnicos de la solución bajo análisis, con el fin de identificar los recursos tangibles que pueden destinarse a la realización de una amenaza determinada. Con esta

² La Corporación MITRE fue constituida en 1958 como una compañía privada sin fines de lucro para proporcionar orientación técnica y de ingeniería al gobierno federal norteamericano. Fuente: <https://www.mitre.org/about/our-history>

información se puede tener una mayor claridad en la comprensión de las oportunidades que un atacante puede tener contra los activos de un entorno objetivo.

- *Descomponer el sistema* – En este paso el sistema analizado se divide en componentes individuales que pueden ser atacados de forma única por un atacante. Este ejercicio permite a un adversario descomponer el sistema objetivo en partes para identificar la mejor forma para atacarlo.

- *Análisis de amenazas* – Esta parte del modelo, considerando la etapa anterior, establecen las razones del por qué y cómo se pueden realizar los ataques al sistema. Para ello se desarrollan preguntas orientadoras que ayuden a visualizar los motivos que hay detrás del ataque al entorno del sistema.

- *Conocimiento de vulnerabilidades* – En este punto del proceso, considerando la información recabada en los pasos previos, se identifican las fallas de diseño o funcionalidad de cada uno de los componentes del sistema, ejercicio que requiere experiencia técnica y experticia práctica que permita identificar las vulnerabilidades propias de sistema objetivo y sus relaciones.

- *Construir el árbol de ataques* – El objetivo de esta etapa se centra en determinar la viabilidad de materializar las vulnerabilidades identificadas en el paso anterior. El éxito de este paso está en la capacidad del profesional que adelanta las pruebas de vulneración para demostrar que las debilidades identificadas son realmente explotables.

- *Análisis de riesgos e impactos* – Esta última fase el modelador de amenazas toma los resultados de la fase anterior y cuantifica los índices de probabilidad de éxito en algunos de los ataques definidos, con el fin de establecer el nivel de riesgo de exposición que tiene el sistema, así como los impactos en sus objetivos de negocio definidos previamente.

Adelantar un ejercicio de análisis de amenazas y vulnerabilidades de un sistema de información o aplicación utilizando P.A.S.T.A, ofrece una visual detallada de sus interacciones, las implicaciones técnicas y de negocio que son claves tener en cuenta y los impactos derivados de la posible materialización de un evento no deseado. En esta dinámica deben participar equipos de trabajo de las áreas afectadas y los profesionales de seguridad con el fin de establecer una vista común de los retos que implica el sistema y sus posibles fallas de identificadas.

C. Attack Trees

Los árboles de ataque son esencialmente diagramas que representan ataques a un sistema en forma de árbol. La raíz del árbol es el objetivo del ataque, y las hojas son las formas de lograr ese objetivo. Cada meta se representa como un árbol separado. Por lo tanto, el análisis de amenazas del sistema produce un conjunto de árboles de ataque. Para tener diferentes opciones de ataque se incorporan nodos “AND” para representar los pasos requeridos para concretar el ataque, y los “OR” para indicar alternativas para conseguir el resultado esperado por el agresor [9].

Adelantar un análisis con esta propuesta metodológica, demanda un conocimiento detallado del sistema que se analiza, dado que no se ofrece mayor detalle sobre submetas, ataques o riesgos que se pueden materializar. Por lo general, esta estrategia de modelaje de amenazas se usa en conjunto con otras, con el fin de poder comprender con detalle la interacción del sistema que se analiza y las implicaciones de seguridad de sus diferentes componentes.

D. Cyberkill Chain

Esta propuesta de modelaje del adversario consta de siete pasos en los cuales se analiza tanto la postura del adversario como la del defensor. De lo anterior, resulta un ejercicio complementario para establecer posibles marcos de actuación que se pueden resolver bien, desde la implementación o actualización de tecnología, pasando por la gestión de los procesos de negocio y su seguridad, la revisión de la cultura organizacional o incluso, desde la generación de escenarios posibles que reten las condiciones vigentes de seguridad y control de la organización.

Las etapas son: [10]

1. Reconocimiento: exploración intencional del objetivo para identificar posibles vulnerabilidades.

2. Militarización: el adversario crea código malicioso o condiciones particulares adaptadas a las debilidades de los objetivos.

3. Entrega: el adversario ubica el código malicioso o configura el escenario en el objetivo.

4. Explotación: se ejecuta el código malicioso o se materializa el escenario estudiado según el plan del adversario.

5. Instalación: la condición adversa se enraíza y conecta en el contexto del objetivo.

6. Comando y control: el código malicioso se comunica con los sistemas del adversario y se crea una condición de control remoto.

7. Acción sobre los objetivos: el código malicioso realiza la acción planeada o el escenario desarrolla y materializa los efectos deseados.

Asumir un enfoque desde el adversario, como la cadena *Cyber Kill*, permite no solo retar los conocimientos y prácticas estándares generalmente adoptadas en las organizaciones, sino que aumenta su capacidad para entender y responder de manera dinámica a las acciones no autorizadas de terceros que quieran resquebrajar la confianza de sus clientes en su entorno de operaciones y desarrollo de actividad comercial.

E. MITRE ATT&CK

De manera general se puede expresar que la propuesta ATT&CK es un modelo de comportamiento que consiste en los siguientes componentes básicos: [11]

- Táctica, que denota objetivos tácticos de los adversarios a corto plazo durante un ataque.

- Técnicas, donde se describen los medios por los cuales los adversarios logran sus metas tácticas.

- Los usos documentados de las técnicas de los

adversarios, y otros metadatos relevantes asociados con las técnicas.

Este modelo se puede utilizar para: [11]

- *Simular al adversario* – Establecer escenarios para probar y verificar las contramedidas instaladas en las organizaciones, frente a técnicas concretas de los adversarios y sus posibles impactos.

- *Aplicar la lógica del adversario* – Asumir el papel de un agresor sin utilizar información de amenazas conocidas, con el fin de desarrollar una operación sin ser detectado, para mostrar el impacto de una operación exitosa y evaluar la capacidad de detección y reacción de una organización frente a estos eventos.

- *Desarrollar analítica de comportamiento* - Usarlo como una herramienta para construir y probar análisis de comportamiento para detectar actividad potencialmente maliciosa dentro de un ambiente y establecer acciones concretas frente a las mismas.

- *Valorar brechas defensivas* – Considerando un modelo de adversario concreto centrado en el comportamiento, validar las herramientas, el monitoreo y mitigación de brechas en las medidas defensivas existentes dentro de la empresa de una organización. Las brechas identificadas configuran una forma de priorizar las inversiones para la mejora del programa de seguridad.

- *Enriquecer la inteligencia de amenazas* – Permite a la organización entender y documentar los perfiles de los grupos adversarios desde una perspectiva de comportamiento que es agnóstica de las herramientas que el grupo pueda utilizar.

El uso de cualquiera de estas propuestas para modelar amenazas y adversarios establece un marco general de acción que permite a los analistas de seguridad de la información ir más allá de la vista tradicional de controles y abrirse a un ejercicio más detallado y relacional, que lo habilita para comprender mejor los riesgos emergentes en sus entornos particulares. Las diferencias entre ellas se encuentran en la aplicación de estas, las cuales demandan esfuerzos particularmente intensivos en dedicación y recursos, con el fin de lograr el objetivo deseado.

Lo anterior implica que seleccionar alguno de ellos, exige conocer la agilidad de la solución requerida, sus tiempos de despliegue, los diferentes equipos de trabajo involucrados, así como el apetito de riesgo corporativo establecido por la alta gerencia, con el fin de identificar el enfoque que mejor se ajusta a la necesidad de la organización. A manera de resumen podemos detallar en la tabla 1, cada una de estas propuestas con sus características y limitaciones.

Tabla 1.

Resumen de características y limitaciones de las propuesta para modelar amenazas

Propuesta metodológica	Características	Limitaciones
STRIDE	<ul style="list-style-type: none"> • Fácil de usar • Focaliza la estrategia de mitigación • Uno de los más usados 	<ul style="list-style-type: none"> * Demanda alto consumo de tiempo y recursos * Requiere conocimiento detallado del sistema a modelar
P.A.S.T.A	<ul style="list-style-type: none"> • Focaliza la estrategia de mitigación • Motiva la colaboración entre los participantes • Facilita el plan priorizado de mitigación 	<ul style="list-style-type: none"> * Demandante en los detalles del sistema que se analiza * Exige documentación detallada de las partes del sistema y sus riesgos
Attack trees	<ul style="list-style-type: none"> • Permite ver con claridad las posibles fallas del sistema • Fácil de usar • Identifica las estrategias de mitigación relevantes 	<ul style="list-style-type: none"> * Requiere conocimiento detallado del sistema para su análisis * No ofrece orientación sobre riesgos, fallas o problemas a analizar
Cyberkill Chain	<ul style="list-style-type: none"> • Permite comprender los pasos del atacante • Establece una vista del adversario y sus acciones • Habilita a la organización para reconocer actividades maliciosas 	<ul style="list-style-type: none"> * Requiere de conocimiento experto * Se pueden presentar conflictos de lenguaje entre especialistas técnicos de los sistemas bajo análisis y las personas de las áreas de negocio
MITRE ATT&CK	<ul style="list-style-type: none"> • Detalla el comportamiento del atacante • Establece con claridad las técnicas y tácticas que puede usar • Basado en conocimiento cierto de eventos y amenazas materializadas 	<ul style="list-style-type: none"> * Toma tiempo la caracterización del perfil requerido * Asume un conocimiento técnico requerido para comprender el patrón del adversario

Fuente: Elaboración propia.

III. MODELO SOCIA. UNA PROPUESTA CONCEPTUAL PARA MODELAR EL ADVERSARIO

Los modelos previamente revisados establecen una serie de condiciones y características que por lo general demandan pasos detallados y procedimientos específicos para lograr los

objetivos trazados en el modelamiento de las amenazas y de los adversarios. En este sentido, aplicar cualquiera de ellos, exige una planeación detallada, entregables concretos y tiempos definidos para lograr esa visión novedosa y emergente que revele los puntos ciegos en la evaluación de vulnerabilidades y brechas de seguridad.

En este entendido, se hace necesario contar con una herramienta liviana, sencilla, efectiva y funcional, que sin pretender desarrollar los alcances que tienen las propuestas analizadas previamente, si ofrezca una forma ágil de lograr un ejercicio base que permita entender el adversario, no como un elemento abierto en un escenario, sino como una realidad evidente y tangible dentro de la dinámica de los procesos, con un mínimo de variables a revisar. Considerando lo anterior, es posible plantear una reflexión enriquecida con los participantes claves del proceso de negocio y los sistemas de información que se quieren analizar.

Siguiendo las reflexiones de Do, Martini y Raymond Choo [12] relacionadas con el papel del adversario en las investigaciones aplicadas en seguridad, y las consideraciones del *Common Sense Security Framework*³ (CSSF), se han identificado cinco (5) variables claves para desarrollar una propuesta metodológica para modelar el atacante denominada SOCIA. SOCIA es una apuesta conceptual de uso ágil para utilizar en el contexto corporativo, con el fin de crear conciencia situacional [13] y reflexiones prospectivas sobre posibles adversarios que pueden tener las organizaciones. Para lograrlo, se parte de la revisión de situaciones previamente materializadas tanto a nivel nacional como internacional, que permitan una visión sistémica de los retos que plantea un atacante, y la participación de diferentes perfiles de colaboradores en la empresa [14,17].

SOCIA es el acrónimo que vincula cinco variables, a saber: Supuestos, Objetivos, Capacidades, Impactos y Aprendizajes (figura 1). A continuación, se detallan cada una de estas variables que configuran una forma de modelar posibles adversarios en el contexto de las organizaciones modernas, considerando la estrategia metodológica del CSSF, de utilizar tres (3) elementos claves para contextualizar el tema, así como sus respectivas preguntas orientadoras.

Figura 1. Modelo SOCIA. Fuente: Elaboración propia

A. Supuestos

Esta primera variable establece las consideraciones básicas de las condiciones y perfil de adversario. En este punto se busca conocer un poco el contexto donde el adversario se mueve, sus conocimientos y recursos disponibles, y para ello, se establecen los siguientes tres (3) elementos con sus preguntas claves:

- Entorno: Interno/Externo - ¿Dónde puede estar ubicado el adversario: dentro o fuera?
- Recursos: Accesos/Equipo - ¿Tiene accesos disponibles bien sea físicos o lógicos, y cuenta con el equipo necesario para lograr sus propósitos?
- Conocimiento: Alto/Medio/Bajo - ¿El adversario cuenta con los conocimientos técnicos y prácticos requeridos para concretar sus acciones no autorizadas?

B. Objetivos

Esta segunda variable busca conocer las motivaciones y datos que son de interés del adversario. En este momento se indaga sobre qué tipo de datos son realmente de interés por parte del atacante, y ver si es posible su monetización. Es claro que no siempre el agresor busca un lucro económico, sino que sus motivaciones pueden ser políticas o ideológicas. Los elementos claves y sus preguntas son:

- Motivación: ¿Por qué? - ¿Cuál es la motivación del adversario para atacar a la organización?
- Activo: ¿Qué tipo de datos? - ¿Qué tipo de datos pueden ser de su interés?
- Monetización: ¿Cuánto puede costar? - ¿Esta información se puede monetizar rápidamente en el mercado?

C. Capacidades

Esta tercera variable revela los patrones de aprendizaje/desaprendizaje que el atacante tiene para producir un daño. En este segmento se evalúa la acción del agresor, cómo se apalanca para concretar sus acciones, y que tipo de afectación ha logrado. Para ello, se detallan a continuación los elementos claves y sus preguntas:

³ Detalles en: <https://commonsenseframework.org/>

- Acción: Pasiva/Activa - ¿La actuación del adversario será pasiva o activa?
- Plataforma: Local/Ecosistema - ¿Sus acciones estarán apalancadas localmente o con apoyo de un ecosistema público?
- Afectación: Baja/Media/Alta - ¿El nivel de afectación que puede generar es alto, medio o bajo?

D. Impactos

Esta cuarta variable revisa las consecuencias concretas que el adversario puede ocasionar con sus capacidades. Es un ejercicio de mirar hacia el interior de la empresa donde se pueden ocasionar las perturbaciones y pérdidas que afecten la organización a nivel del negocio, los procesos y la infraestructura. Los elementos claves y sus preguntas orientadoras son:

- Negocio: Parcial/Total - ¿El negocio puede sufrir afectaciones parciales o totales?
- Procesos: Parcial/Total - ¿Los procesos pueden ser afectados de forma parcial o total?
- Infraestructura: Parcial/Total - ¿La infraestructura se puede comprometer parcial o totalmente?

E. Aprendizajes

La quinta y última variable explora las lecciones aprendidas, las acciones de remediación y la actualización de la postura de seguridad que la organización debe incorporar, para ajustar sus mecanismos de defensa y tratar de anticipar nuevos eventos en el futuro. Para ello, se detallan a renglón seguido los elementos claves y sus preguntas:

- Lecciones: Aprendidas/por aprender - Frente a un atacante con estas características, ¿qué lecciones por aprender tenemos?
- Remediación: Negocio/Proceso/Infraestructura - ¿Tenemos claros cómo deben ser los procesos de contención y remediación del negocio, el proceso y la infraestructura?
- Postura: Defender/Anticipar - ¿Cómo debe cambiar la postura de seguridad de la organización: defender o anticipar?

Estas cinco (5) variables, si bien no buscan ser exhaustivas ni detalladas en su desarrollo, sí facilitan una conversación abierta e incluyente desde los diferentes actores de la empresa, con el fin de revelar posibles puntos ciegos en su dinámica de la seguridad y ciberseguridad, a fin de que se posibilite la generación de una consciencia colectiva sobre los posibles adversarios y la manera como pueden afectarla; y de la misma forma, ver estrategias de defensa y anticipación distintas, que enriquezcan la batería disponible de estrategias de protección de los activos de información críticos de las organizaciones [27].

IV. APLICACIÓN DEL MODELO SOCIA. UNA VISIÓN PRÁCTICA DE SU USO

El Modelo SOCIA recientemente se utilizó en un ejercicio académico de revisión y análisis del escenario de amenazas

digitales emergentes de una entidad financiera en Colombia, realizado con los profesionales del área de la auditoría interna. En el desarrollo del taller de aplicación los auditores con diferentes profesiones como Contadores Públicos, Ingenieros de Sistemas, Administradores de Empresas, entre otros, se distribuyeron en tres grupos de trabajo interdisciplinarios con el fin de estudiar tres (3) casos de ciberataques internacionales. El objetivo fue conceptualizar las posturas de los atacantes y concretar reflexiones prácticas al interior de la dinámica de la entidad y su factibilidad, las cuales socializaron al final del ejercicio.

Para ello, se diseñó un formato de trabajo (ver figura 2), que integra las variables del modelo y sus elementos asociados, en el que se recogieron, con el apoyo del facilitador del ejercicio, las inquietudes y conversaciones que surgieron en cada equipo de trabajo durante el estudio del caso, cuya información fue proporcionada y complementada mediante búsquedas en internet.

SOCIA	Nombre del Caso:
Supuestos (Configura el adversario y su entorno)	ENTORNO: RECURSOS: CONOCIMIENTO:
Objetivos (Establece las motivaciones del adversario)	MOTIVACIÓN: ACTIVO: MONETIZACIÓN:
Capacidades (Identifica el nivel de daño que puede causar)	ACCIÓN: PLATAFORMA: AFECTACIÓN:
Impactos (Analiza las afectaciones claves que puede ocasionar)	NEGOCIO: PROCESOS: INFRAESTRUCTURA:
Aprendizajes (Revisa algunos puntos ciegos en el modelo de seguridad de la empresa)	LECCIONES: REMEDIACIÓN: POSTURA:

Figura 2. SOCIA. Formato de trabajo. Fuente: Elaboración propia.

Uno de los casos revisados durante el ejercicio, fue el ciberataque realizado recientemente al Banco Central de México – BANXICO, en el cual terceros no identificados y altamente documentados en el sistema de pagos interbancarios – SPEI, lograron desarrollar una acción coordinada con diferentes actores para robar dinero de bancos comerciales en este país.

A manera de ejemplo se presenta a continuación el resultado obtenido por uno de los equipos de trabajo (ver figura 3), así como algunas de sus reflexiones realizadas una vez concluida su presentación sobre el caso, siguiendo los elementos propios del Modelo SOCIA.

SOCIA	BANXICO
Supuestos (Configura el adversario y su entorno)	ENTORNO: Adversario Externo RECURSOS: Cuenta con equipo necesario para actuar y apoyo para desplegar la acción no autorizada. CONOCIMIENTO: El adversario tiene un nivel de conocimiento especializado del sistema de pagos
Objetivos (Establece las motivaciones del adversario)	MOTIVACIÓN: Económica ACTIVO: Cuentas de bancos y datos de correntistas MONETIZACIÓN: Tanto como las transferencias no autorizadas que se logren.
Capacidades (Identifica el nivel de daño que puede causar)	ACCIÓN: Activa sobre el sistema de pagos PLATAFORMA: Desarrollo local AFECTACIÓN: Alta
Impactos (Analiza las afectaciones claves que puede ocasionar)	NEGOCIO: Parcial PROCESOS: Total INFRAESTRUCTURA: Parcial
Aprendizajes (Revela algunos puntos ciegos en el modelo de seguridad de la empresa)	LECCIONES: Acciones coordinadas con los bancos/Mejora de la gestión de incidentes REMEDIACIÓN: Análisis de vulnerabilidades / Pruebas conjuntas POSTURA: Supera la postura preventiva.

Figura 3. SOCIA. Resumen del resultado - Caso BANXICO. Fuente: Elaboración propia

Luego de presentar este análisis, los diferentes miembros del equipo hicieron comentarios y afirmaciones sobre lo revisado que se pueden resumir como sigue:

- Es posible que podamos tener un atacante como estos y, por tanto, nos exige un ejercicio de coordinación con los supervisores del sector, así como con el Banco Central.
- Es necesario adelantar simulaciones y ejercicios de este tipo, para prepararnos, junto con el sector en general, lo cual demanda enriquecer la postura de seguridad y control actual de la entidad.
- No podemos confiarnos en los mecanismos de seguridad y control que tenemos instalados en este momento, es necesario crear condiciones adversas dentro de la plataforma actual, para ver cómo reacciona y qué puntos ciegos tenemos a la fecha que son relevantes para asegurar la operación de la institución.

De otra parte, los equipos interdisciplinarios que se conformaron para desarrollar el ejercicio utilizando SOCIA reconocieron puntos de vista distintos, creando nuevas oportunidades de actividades conjuntas, con estrategias complementarias, que superan las aproximaciones exclusivamente tecnológicas que se tienen a la fecha para adelantar los planes de auditoría cuando se trata de los temas de seguridad y control en la entidad.

Estas reflexiones y otras adicionales, como resultado de los otros equipos conformados, establecieron referentes distintos de la mirada actual de la auditoría, considerando elementos que no estaban vinculados a la fecha en su plan de trabajo. Adicionalmente, fue un ejercicio para retar sus prácticas actuales basadas en estándares y marcos de trabajo reconocidos, donde se hicieron evidentes las limitaciones inherentes de los mismos respecto de entornos inciertos e inestables como los que actualmente tienen las organizaciones modernas.

V. CONCLUSIONES

En el ejercicio cotidiano de proteger y asegurar las organizaciones, las prácticas de seguridad y control guiadas por los estándares conocidos ha sido la norma sobre la cual, tanto las áreas de seguridad/ciberseguridad, como las de auditoría, han fundado sus diferentes acciones para generar un

marco de confianza regulado cimentado sobre controles. Bajo este entendido, las empresas han logrado movilizar iniciativas de negocio innovadoras que habilitan a sus clientes, para lanzarse a concretar una interacción cada vez más digital y con menos intervención humana [15, 20].

No obstante lo anterior, la evolución de los adversarios y sus inesperadas formas de concretar sus acciones adversas genera tensiones sobre los estándares de seguridad y control vigentes, creando una zona de incertidumbre donde es necesario repensar la manera como se entiende ahora la protección de la información en las empresas [16, 18]. Esto es, habilitar espacios de reflexión basados en los inciertos e inestabilidades del entorno, con la participación de diferentes perfiles de personas en las organizaciones, para encontrar puntos de vista diferentes a las certezas y definiciones que ofrecen las buenas prácticas internacionales.

Incluir al adversario como un nuevo elemento dentro de las reflexiones de protección de los activos digitales de las empresas, abre una ventana de aprendizaje y desaprendizaje, que busca crear espacios complementarios de discusión, que permitan contrastar las lecturas de los riesgos conocidos provistas por los estándares, frente a las posibilidades y escenarios alternativos que ofrece una propuesta metodológica como SOCIA, donde el agresor, lejos de ser un desconocido para el análisis, se convierte en materia de estudio para crear una consciencia situacional sobre posibles puntos ciegos que actualmente pueden estar vigentes en la dinámica de la empresa [28].

Vincular al atacante como materia de estudio, no es una invitación ni sugerencia para que las áreas de seguridad/ciberseguridad, o auditoría, se conviertan en los mismos verdugos de las organizaciones, sino una manera distinta para identificar los pasos de los agresores (bien sean internos o externos), caminar en la dinámica de su mente y motivaciones, con el fin de defender y anticipar acciones concretas que apoyen su preparación frente a eventos inciertos o inesperados, que permanecen latentes en la ejecución de sus procesos actuales sin signos de manifestación concretos [29].

SOCIA como propuesta metodológica se basa en la dinámica social y de negocio de la organización, que sin entrar en los detalles tecnológicos del ataque analizado, permite conectar diversas vistas de los participantes, creando un lenguaje común para elaborar un entendimiento de la dinámica del adversario, no desde su habilidad técnica exclusivamente, sino desde sus técnicas y estrategias para configurar la acción no autorizada, aumentando la sensibilización de las personas sobre las capacidades de los agresores y sus impactos en la promesa de valor de la compañía.

En consecuencia, SOCIA establece una forma distinta e incluyente para visualizar y caracterizar los posibles adversarios que puede tener una empresa y en este ejercicio,

comenzar a construir nuevas capacidades de defensa y anticipación, que permita a las organizaciones desarrollar escenarios, prototipos y simulaciones [21] que la ubiquen en una posición menos reactiva frente a las situaciones imprevistas, y la proyecten como una comunidad resiliente, experimentada en la atención de incidentes, que sabe que el adversario es inteligente y hábil, y que tarde o temprano tendrá éxito.

AGRADECIMIENTOS

El autor agradece a los doctores Jesús Vásquez Gómez, Especialista de Tecnología de Información del Banco Central de México y Gabriela María Saucedo Meza, Docente de la Universidad Militar Nueva Granada de Colombia, por sus valiosos y acertados comentarios que permitieron afinar las reflexiones de este artículo.

REFERENCIAS

- [1] Donaldson, S., Siegel, S., Williams, C. & Aslam, A. (2015). *Enterprise Security. How to build a successful cyberdefense program against advanced threats*. New York, USA: Apress
- [2] Sieber, S. & Zamora, J. (2018). The Cybersecurity Challenge in a High Digital Density World. *European Business Review*. Recuperado de: <https://www.europeanbusinessreview.com/the-cybersecurity-challenge-in-a-high-digital-density-world/>
- [3] Cano, J. (2019). Analyst and Adversary. Deconstructing the “Imaginary” of Security and Cybersecurity Professionals. *ISACA Journal*. 4. 48-53.
- [4] Tounsi, W. & Rais, H. (2017). A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Computers & Security*, 72. 212-233. doi:10.1016/j.cose.2017.09.001.
- [5] Cano, J. (2017). The AREM Window: A Strategy to Anticipate Risk and Threats to Enterprise Cyber Security. *ISACA Journal*. 5.
- [6] Shostack, A. (2014). *Threat Modeling: Designing for Security*. Indianapolis, IN. USA: John Wiley & Sons.
- [7] Khan, R., McLaughlin, K., Laverty, D., & Sezer, S. (2018). STRIDE-based Threat Modeling for Cyber-Physical Systems. In 2017 IEEE PES: Innovative Smart Grid Technologies Conference Europe (ISGT-Europe): *Proceedings IEEE*. doi: 10.1109/ISGTEurope.2017.8260283
- [8] UcedaVélez, T. & Morana, M. (2015). *Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis*. Hoboken, NJ. USA: John Wiley & Sons.
- [9] Schneier, B. (1999). Attack trees. Modeling security threats. *Dr. Dobbs Journal*. December. Recuperado de: https://www.schneier.com/academic/archives/1999/12/attack_trees.html
- [10] Hutchins, E., Cloppert, M. & Amin, R. (2011). Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. *White Paper*. Lockheed Martin. Recuperado de: <https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf>
- [11] Strom, B., Applebaum, A., Miller, D., Nickels, K., Pennington, A. & Thomas, C. (2018). MITRE ATT&CK™: Design and Philosophy. *MITRE Product*. Recuperado de: <https://www.mitre.org/publications/technical-papers/mitre-attack-design-and-philosophy>
- [12] Do, Q., Martini, B., & Raymond Choo, K. K. (2018). The Role of the Adversary Model in Applied Security Research. *Computers & Security*. 81, 156-181. doi:10.1016/j.cose.2018.12.002
- [13] Franke, U. & Brynielsson, J. (2014). Cyber situational awareness – a systematic review of the literature, *Computers & Security*. 46. 18-31. doi: 10.1016/j.cose.2014.06.008.
- [14] Cano, J. (2019). Ciberriesgo. Aprendizaje de un riesgo sistémico, emergente y disruptivo. *Revista SISTEMAS*. Asociación Colombiana de Ingenieros de Sistemas. 63-73. Doi: 10.29236/sistemas.n151a5
- [15] Accenture (2019). Cyber resilience for industry X.0 in Europe. Agile cybersecurity in the age of the Industrial Internet of Things. Recuperado de: <https://acntu.re/2TvkQYy>
- [16] Campbell, N. (2017). Cyber Security Is A Business Risk, Not Just An IT Problem. *Forbes*. Recuperado de: <https://www.forbes.com/sites/edelmantechnology/2017/10/11/cyber-security-is-a-business-risk-not-just-an-it-problem/>
- [17] Carlton, M., Levy, J. & Ramim, M. (2019). Mitigating cyber attacks through the measurement of non-IT professionals’ cybersecurity skills. *Information & Computer Security*, 27(1), 101-121. Doi: 10.1108/ICS-11-2016-0088
- [18] Raban, Y. & Hauptman, A. (2018). Foresight of cyber security threat drivers and affecting technologies. *Foresight*. Doi: 10.1108/FS-02-2018-0020
- [19] Mossburg, E., Gelinne, J. & Calzada, H. (2017). Beneath the Surface of a cyberattack. A deeper look at business impact. *Deloitte*. Recuperado de: <https://www2.deloitte.com/us/en/pages/risk/articles/hidden-business-impact-of-cyberattack.html>
- [20] Weill, P., Apel, T., Woerner, S. & Banner, J. (2019). It Pays to Have a Digitally Savvy Board. *Sloan Management Review*. Recuperado de: <https://sloanreview.mit.edu/article/it-pays-to-have-a-digitally-savvy-board/>
- [21] Cano, J. (2018). Repensando los fundamentos de la gestión de riesgos. Una propuesta conceptual desde la incertidumbre y la complejidad. *Revista Ibérica de Tecnología y Sistemas de la Información*. E15. Abril. 76-87.
- [22] Shevchenko, N., Chick, T., O’Riordan, P., Scanlon, T. & Woody, C. (2018). Threat modeling: a summary of available methods. *SEI Carnegie Mellon University*. Recuperado de: https://resources.sei.cmu.edu/asset_files/WhitePaper/2018_019_001_524597.pdf
- [23] Woods, D., Dekker, S., Cook, R., Johannesen, L. & Sarter, N. (2010). *Behind human error*. Second Edition. Farnham, Surrey. England: Ashgate Publishing Limited
- [24] Kumar, T., Porambage, P., Ahmad, I., Liyanage, M., Harjula, E. & Ylianttila, M. (2018). Securing Gadget-Free Digital Services. *IEEE Computer*. 66-77. Doi: 10.1109/MC.2018.2876017
- [25] EY (2018). Is cybersecurity more than protection?. EY Global Information Security survey 2018-19. *Reporte*. Recuperado de: [https://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2018-19/\\$FILE/ey-global-information-security-survey-2018-19.pdf](https://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2018-19/$FILE/ey-global-information-security-survey-2018-19.pdf)
- [26] Higuera, J. (2017). La gestión de la ciberseguridad como estrategia: el peligro de la vulnerabilidad y cómo mitigarla. *Harvard Deusto*. 12-19.
- [27] Sabillón, R. & Cano, J. (2019). Auditorías en Ciberseguridad: Un modelo de aplicación general para empresas y naciones. *Revista Ibérica de Sistemas y Tecnologías de Información*. 32. 33-48.
- [28] Roberts, S. & Brown, R. (2017). *Intelligence-Driven Incident Response. Outwitting the Adversary*. Sebastopol, CA. USA: O’Reilly
- [29] Ahmad, Z., Ong, T., Liew, T. & Norhashim, M. (2019). Security monitoring and information security assurance behaviour among employees: An empirical analysis. *Information & Computer Security*. Doi: 10.1108/ICS-10-2017-0073
- [30] Thakur, K., Tseng, J. & Hayajneh, T. (2019). Cyber Security in Social Media: Challenges and the Way Forward. *IEEE IT Professional*. 21(2). 41-49. Doi: 10.1109/MITP.2018.2881373.

Jeimy J. Cano M. 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 in Business Administration por Newport University, CA. USA y Ph.D en Educación por la Universidad Santo Tomás en Colombia. Profesor universitario a nivel de pregrado, especialización, maestría y doctorado en Colombia y varios países de Latinoamérica en temas como computación forense, evidencia digital, gobierno y gestión de la seguridad de la información, gerencia de sistemas de información, criminalidad informática, auditoría de TI, ciberseguridad y protección de datos personales desde 1996 a la fecha. ORCID: <https://orcid.org/0000-0001-6883-3461>