Juegos de guerra

Un ejercicio de construcción conjunta en ciberseguridad y seguridad de la información.

Jeimy J. Cano M., Ph. D., CFE.

Introducción

En un contexto geopolítico inestable, con amenazas digitales inciertas y nuevos competidores creando incertidumbres globales, las organizaciones deben avanzar rápidamente en espacios de construcción colectiva que permitan crear capacidades inexistentes frente a escenarios que aún no ocurren (Cano, 2017).

Bajo esta perspectiva los conceptos de ciberseguridad y seguridad de la información, comienzan a reconstruir sus fronteras naturales y transitan hacia prácticas, algunas desconocidas, sobre contextos digitalmente modificados, en los que cualquier evento puede ocurrir y afectar las condiciones normales de la operación de una empresa. Posiblemente, esto implica desconectar y repensar conceptos sobre los cuales los estándares conocidos han sido planteados, para encontrar nuevas oportunidades que construyan un nuevo normal de "confianza" para las empresas en una sociedad tecnológicamente moldeada.

Para lograr lo anterior, tanto la ciberseguridad como la seguridad de la información, temáticas complementarias en sí mismas, deben crear un mercado propio, que haga nuevos trazados sobre un territorio de volatilidades digitales, con el fin de encontrar distinciones que permitan a las organizaciones y a las personas establecer sus propios fundamentos de la lectura de la protección, en el conjunto de expectativas y logros que se pretenden lograr, anticipar y desarrollar para conquistar un nuevo lugar en la dinámica de los negocios actuales.

Esto supone que la ciberseguridad y la seguridad de la información dejen de ser aspectos solitarios de las empresas, dominios controlados por un conocimiento especializado, para convocar la sabiduría del negocio y de sus participantes, habida cuenta que su visión en el terreno ofrece aspectos de

la realidad que, por lo general, superan la percepción particular de un analista de seguridad o ciberseguridad.

En este sentido, la práctica de los "juegos de guerra" (en inglés *war games*) establece una oportunidad para encontrar los diferentes puntos de vista de la dinámica de la organización con la lectura de los analistas de seguridad y ciberseguridad, orientados a comprender y construir en conjunto, las acciones requeridas para responder táctica y estratégicamente a la experiencia de un ciberataque, o mejor, a un escenario de negocio donde se compromete la promesa de valor de la compañía en un entorno digitalmente modificado.

Aunque esta práctica no es nueva en el escenario global, como quiera que ha sido utilizada en entornos de defensa nacional por algunas fuerzas militares del mundo (Perla, 1990), sí es una nueva apuesta que marca un estado de madurez en la comprensión de los escenarios tecnológicamente modificados de las empresas, en las que tanto los directivos como las personas de la línea de operación, además de los especialistas en seguridad y ciberseguridad, participan para crear una visión simulada de un ciberataque con información incompleta, que pruebe las capacidades de la organización para enfrentar este tipo de situaciones digitales adversas.

Juegos de guerra: una apuesta de construcción conjunta

En el contexto militar los juegos de guerra suponen un reconocimiento de los actores en conflicto, una perfilación de las capacidades del oponente, un territorio que se debe dominar y una conquista que se debe concretar. Por lo general, en este escenario las partes entre sí se reconocen y saben qué tiene cada una para concretar golpes certeros sobre los activos estratégico de la otra, por lo cual el combate se convierte en un juego de estrategias para saber usar lo que se tiene, con el fin de tomar ventaja frente a las limitaciones de los otros (Perla, 1990).

En este juego de estrategia, quien logre la mayor ventaja, es decir, logre descifrar la dinámica de su inteligencia, las tácticas de operación de las tropas, inhabilite las posibles armas claves de mayor destrucción y daño e infiltre las mismas operaciones de su oponente, sin que este lo note, tendrá una superioridad militar que doblega y compromete los planes de su enemigo, no solamente en el terreno operativo, sino en la conceptualización y estrategia de guerra.

Esta lectura militar de los juegos de guerra, si bien suena amenazante y clásica frente al reto de la defensa nacional, plantea un desafío de interés para las organizaciones con el fin de concretar estrategias de defensa frente a un entorno asimétrico e incierto, donde existen múltiples intereses comprometidos, actores conocidos y desconocidos, que en cualquier momento pueden crear el escenario específico en el que pueden comprometer las operaciones claves de una empresa.

Por tanto, los "juegos de guerra" en el contexto empresarial establecen momentos de preparación, reflexión y desafío permanente para habilitar la construcción de una capacidad colectiva de comprensión y desaprendizaje organizacional, sobre la realidad de

las amenazas digitales actuales, orientada a establecer y anticipar estrategias y acciones claves que permitan actuar frente a ataques digitales o campañas planeadas por terceros en contra de la dinámica de la empresa, de manera de aumentar la capacidad de resiliencia empresarial necesaria para continuar avanzando sobre mercados inexplorados y crear oportunidades en medio de situaciones inciertas (Bailey, Kaplan y Weinberg, 2012).

Los "juegos de guerra" en las organizaciones establecen un nivel de compromiso mayor en sus ejecutivos, como quiera que la comprensión de la dinámica de los negocios y sus implicaciones, dejan de estar en los niveles tradicionales de riesgo empresarial y se enriquecen desde la perspectiva de los ecosistemas digitales donde opera la empresa. Esto es, los directivos comienzan a incorporar la distinción de los productos y servicios digitalmente modificados y sus impactos en los diferentes grupos de interés.

Cuando los "juegos de guerra" se constituyen en una práctica permanente de la empresa, la organización permanece en "modo radar" (Prize, 2015); es decir, explorando e identificando aspectos de su entorno digital para capitalizar como oportunidad o reconociendo posibles amenazas para actuar de manera anticipada y aumentar su capacidad de respuesta ágil y efectiva, según se materialicen los impactos de un riesgo desconocido o no identificado.

Juegos de guerra: una aproximación metodológica

Desarrollar un ejercicio de "juegos de guerra" demanda una serie de pasos preliminares, semejantes a la construcción de un escenario, pero diferenciada, en la medida en que se priorizan las acciones contrarias, desde los diferentes puntos de vista de los actores invitados al ejercicio y las capacidades requeridas, para dar cuenta de la situación adversa.

De acuerdo con Bailey, Kaplan y Weinberg (2012) es importante considerar las siguientes preguntas con el fin de contextualizar el ejercicio de "juegos de guerra":

- ¿Puede la organización identificar y valorar rápidamente una brecha de seguridad?
- ¿Puede la organización tomar decisiones efectivas para contener la brecha identificada?
- ¿Puede comunicar efectivamente la brecha identificada a todos sus grupos de interés?
- ¿Puede ajustar rápidamente las estrategias y tácticas de negocio con ocasión de la brecha identificada?
- ¿Puede la organización actuar en conjunto con aliados estratégicos de forma efectiva frente a la brecha identificada?

Basado en estas primeras consideraciones, se plantean, siguiendo las indicaciones metodológicas de la práctica de Intel (Casey y Willis, 2008), dos escenarios, el "más probable" y el de "mayor impacto o daño". Cada escenario planteado contiene al menos los siguientes elementos:

- Un agente que provoca el impacto o daño (por ejemplo, hacktivista pa-

trocinado por un estado, crimen organizado, actor no identificado, empleado interno).

- Habilidades requeridas (por ejemplo, ingeniería social, *malware*, espionaje, vulnerabilidad conocida o desconocida).

- Objeto del ataque (por ejemplo, cuenta de correo electrónico, cuentas de redes sociales, cuentas financieras, datos personales).

- Objetivo del ataque (por ejemplo, robo de información personal, robo de propiedad intelectual, daño en los datos, daño en la imagen, pérdida financiera, interrupción del servicio).

- Indicadores del entorno (por ejemplo, noticias sobre ataques similares, casos semejantes procesados por las autoridades, recientes hallazgos académicos o de la industria sobre nuevas vulnerabilidades).

Con esta información se procede a escribir una historia que conjugue todos los elementos planteados previamente, con el fin de crear un contexto de reflexión base que permita a los participantes imaginar posibilidades, desde cada uno de sus puntos de vista. En este ejercicio no se desecha ninguna perspectiva ni se restringen posturas de los participantes, como quiera que es de esta forma como se enriquece la historia planteada y los elementos de riesgo o amenaza identificados hasta ese momento (Casey y Willis, 2008).

Luego un facilitador, preferiblemente del área de seguridad o ciberseguridad de la información, compila las diferentes visiones identificadas sobre la historia, establece los enlaces frente a las capacidades claves de la organización y aquellos elementos que no puedan relacionarse con las capacidades actuales, para resaltarlos como fuentes de vulnerabilidad que deben ser estudiados y revisados por la organización, en conjunto con el área de seguridad y ciberseguridad y los ejecutivos de la empresa.

Considerando los dos escenarios planteados, este ejercicio deberá tomar por lo menos dos días de trabajo dedicado (Casey y Willis, 2008), con el fin de documentar y establecer los elementos suficientes para fundamentar el escenario de amenazas emergentes planteados, las vulnerabilidades conocidas o no documentadas, las brechas de capacidad que tiene la empresa frente a los escenarios conocidos y finalmente las acciones de mitigación, preparación o defensa requeridas para actuar y superar las posibles inestabilidades que puedan generar la materialización de dichos escenarios.

Juegos de guerra: cambios de perspectiva

La aplicación de los "juegos de guerra" en el contexto de las prácticas de seguridad de la información y ciberseguridad, establecen un planteamiento disruptivo que supera la visión de controles generales y sobre todo, la de riesgos particulares sobre el tratamiento de la información en la empresa. Este nuevo ejercicio de exploración y respuesta a la incertidumbre del entorno permite a la organización como a la seguridad de la información y a la ciberseguridad:

- Tener el tiempo para pensar y facilitar reflexiones de manera creativa

en torno de los desafíos de un contexto digitalmente modificado.

- Superar los límites de los estándares conocidos, con el fin de desafiar continuamente sus prácticas.

- Dialogar constantemente con el exterior, desconectando lo conocido para enriquecerlo con lo volátil, incierto, complejo y ambiguo.

- Aprender a generar valor más allá de los productos o servicios propios de la organización.

- Mejorar la capacidad de resiliencia de la organización frente a entornos inciertos y volátiles (Adaptado de: Ponti y Ferrer, 2011).

Por tanto, los "juegos de guerra" motivan de forma inteligente el uso de las habilidades emocionales y sociales de los participantes alrededor de los retos de la seguridad y ciberseguridad en entornos digitalmente modificados. Es en palabras de Bailey, Kaplan y Weinberg (2012) un "*mecanismo para establecer la prioridad de los activos a proteger, identificar, superar y cerrar las vulnerabilidades claves, identificar las fallas propias en la capacidad de respuesta ante un evento adverso y construir un tipo de 'memoria con músculo' necesaria para tomar decisiones apropiadas en tiempo real con información limitada*".

Así las cosas, esta práctica establece una forma de cambiar el imaginario de la seguridad de la información y la ciberseguridad que sugiere un espacio de construcción conjunta, donde los participantes se divierten trabajando en un ambiente de motivación, curiosidad y pasión que releva los matices propios de las prácticas de seguridad y control de la organización, no solo en su interior, sino como parte de la dinámica exterior empresarial que forma parte del ecosistema digital del cual es partícipe.

Los "juegos de guerra" no solo revelan problemáticas particulares de las amenazas digitales o impactos en los activos digitales críticos de las empresas, sino que dejan ver otros riesgos propios de los procesos de negocio, impactos no dimensionados sobre grupos de interés y aspectos inexplorados de las relaciones entre los procesos de negocio, que comunican vulnerabilidades o fallas existentes en las áreas corporativas que no se habían identificado (Casey, 2007).

Reflexiones finales

En el contexto empresarial, los "juegos de guerra" establecen una lectura proactiva y de construcción conjunta de las capacidades corporativas para anticipar y responder de la mejor forma a las inestabilidades del entorno de los negocios actuales.

A diferencia del ejercicio que se esboza en el escenario militar, el enemigo en un ambiente volátil, incierto, complejo y ambiguo ya no es conocido y mucho menos sus capacidades o armamento disponibles para comprometer los activos digitales estratégicos de la empresa. En este sentido, la práctica de gestión de riesgos tradicional se debilita, para darle paso a una nueva forma de aumentar la capacidad de visualización y entendimiento de los nuevos patrones de amenazas existentes que pueden afectar las promesas de valor de la empresa para con sus clientes.

En consecuencia, los "juegos de guerra" plantean un ejercicio diferente para motivar estrategias de protección del valor de los activos digitales empresariales, y provocar acciones creativas, orientadas a atender la incertidumbre natural de los entornos de negocios actuales, para concretar puntos de desconexión de los conceptos conocidos, con el fin de incorporar tendencias y rarezas del exterior, que permitan nuevas ganancias teóricas y prácticas en el entendimiento de los retos empresariales al interior.

Los "juegos de guerra" permiten validar concretamente los supuestos propios sobre las prácticas de seguridad y control vigentes en la empresa, con el propósito de hacer una declaración sincera sobre el nivel de exposición de sus activos críticos.

Se trata de comprender y declarar desde la inevitabilidad de la falla, la oportunidad para construir de forma colaborativa una nueva realidad de la protección del valor de la corporación, frente al reto de una acelerada digitalización de productos y servicios.

Los "juegos de guerra" permiten una democratización de la lectura de la protección de los activos digitales, que conjuga las perspectivas de las personas a cargo de los mismos, con la visión especializada de los analistas de seguridad de la información y ciberseguridad. En este ejercicio, no solamente se retan los supuestos de base de la seguridad y control actuales, sino que se habilitan espacios para compartir lecciones aprendidas en otras temáticas, que nutren el ejercicio como una estrategia para recolectar información y motivar analíticas de datos hacia el futuro.

Considerando la acelerada transición hacia la nueva revolución industrial, mediada por la digitalización de productos y servicios (Kane, 2017), para crear nuevas experiencias motivadas en los datos e información recolectada de los diferentes grupos de interés, los ejercicios de "juegos de guerra" igualmente deberán avanzar en sus desarrollos incorporando las posibilidades de simulaciones con el uso de inteligencia artificial, desarrollo de prototipos y juegos de roles que permitan entrenar a los participantes en las decisiones que deben tomar frente a momentos de incertidumbre y confusión total.

Este documento no pretende agotar las reflexiones sobre las nuevas formas de reconocer patrones emergentes en el entorno, pero sí es una excusa académica para pensar de forma diferente sobre el entendimiento de los nuevos desafíos del entorno y cultivar un diálogo creativo hacia el surgimiento de pensamientos no convencionales en seguridad de la información y ciberseguridad, que obliguen una mirada de la realidad a través de una óptica totalmente distinta, superando el temor a lo desconocido y rompiendo las barreras y supuestos de los estándares conocidos.

Referencias

[1] Bailey, T., Kaplan, J. y Weinberg, A. (2012) Playing war games to prepare for a cyberattack. *Mckinsey Quarterly*. July. Recuperado de: http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/playing-war-games-to-prepare-for-a-cyberattack

[2] Cano, J. (2017) El riesgo geopolítico en clave de la seguridad y la ciberseguridad de las empresas modernas. Recuperado

de: https://www.linkedin.com/pulse/el-riesgo-geopol%C3%ADtico-en-clave-de-la-seguridad-y-las-cano-ph-d-cfe

[3] Casey, T. (2007) Threat Agent Library Helps Identify Information Security Risks. *Intel White Paper*. Recuperado de: https://communities.intel.com/servlet/JiveServlet/previewBody/1151-102-1-1111/Threat%20Agent%20Library_07-2202w.pdf

[4] Casey, T. y Willis, B. (2008) Wargames: Serious play that test enterprise security assumptions. *Intel White Paper*. Recuperado de: https://communities.intel.com/docs/DOC-1519

[5] Kane, G. (2017) Digital Maturity, Not Digital Transformation. *Sloan Management Review*. Blog. Recuperado de: http://sloanreview.mit.edu/article/digital-maturity-not-digital-transformation/

[6] Perla, P. (1990) *The art of wargaming: A guide for professionals and hobbyist*. USA: US Naval Institute Press

[7] Ponti, F. y Ferrer, J. M. (2011) *Si funciona, cámbielo. Cómo innovar sin morir en el intento*. Bogotá, D.C, Colombia: Grupo Editorial Norma.

[8] Prize, W. (2015) *1000 ideas para atraer lo que quieras a tu vida*. Madrid, España: Mestas Ediciones.

Jeimy J. Cano M., Ph. D., CFE. *Profesor Asociado, Escuela de Administración, Universidad del Rosario. Ingeniero y Magíster en Ingeniería de Sistemas y Computación de la Universidad de los Andes. Especialista en Derecho Disciplinario de la Universidad Externado de Colombia. Ph. D. en Administración de Negocios de Newport University, CA. USA y Ph. D. (c) en Educación de la Universidad Santo Tomás. Obtuvo un Certificado Ejecutivo en Liderazgo y Administración del MIT Sloan School of Management y es egresado de los programas de formación ejecutiva de Harvard Kennedy School of Government: Liderazgo en el siglo XXI: Agentes globales de cambio y Ciberseguridad: Intersección entre política y tecnología, ambos en Boston, USA. Ha sido reconocido como "Cybersecurity Educator of the year 2016" para Latinoamérica, por Cybersecurity Excellence Awards. Es Examinador Certificado de Fraude – CFE por la ACFE y Cobit5 Foundation Certificate por ISACA. Cuenta con más de 20 años de experiencia como académico y profesional en seguridad de la información, auditoría de TI, forensia digital, delitos informáticos, privacidad y temas convergentes en Colombia y Latinoamérica y más de un centenar de publicaciones en diferentes eventos y revistas nacionales e internacionales.*