Ciberataques

DOI: 10.29236/sistemas.n157a6

¿Impuestos inevitables en la dinámica de una economía digital?

Resumen

En un contexto cada vez más digital y de iniciativas innovadoras con tecnología de información se desarrolla una economía digital que conecta los diferentes actores de la sociedad, con el fin crear nuevos ecosistemas de negocios en los que es posible concretar oportunidades, utilidades y experiencias inéditas para los diferentes grupos de interés. En este sentido, la inseguridad digital, representada en los ciberataques, se configura como un impuesto progresivo que grava la confianza digital de los consumidores y crea zonas inciertas que afectan la dinámica empresarial y la prosperidad económica de las naciones. En consecuencia, este artículo desarrolla una reflexión conceptual alrededor de este nuevo impuesto progresivo, así como algunas ideas para concretar su elusión en un entorno cada vez más digital y tecnológicamente modificado.

Palabras clave

Ciberataques, Ciberseguridad, Ciberriesgo, Confianza digital, Impuestos

Jeimy J. Cano M.

Introducción

En un proceso acelerado de transformación digital por cuenta de la asimetría global provocada por un evento, para muchos predecible, las organizaciones enfrentan un escenario de mayor visibilidad digi-

tal y expansión de operaciones basados en una articulación flexible con terceros de confianza (Cooray & Duus, 2020). En este contexto, la necesidad de abrir sus fronteras para lograr una mayor convergencia de sus productos y consumidores establece nuevos patrones de interacción en los que las aplicaciones móviles, los portales de ventas, los carritos de compras y los códigos QR se convierten en las estrategias más utilizadas.

En este entorno inesperado las empresas implementaron, en poco tiempo y sin verificar, nuevos puntos de conexión en sus infraestructuras, lo que constituye un caldo de cultivo de vulnerabilidades potenciales que los posibles adversarios pueden aprovechar para desestabilizar la estrategia empresarial ajustada, con el fin de mantenerse a flote en medio de las restricciones de movilidad y contacto que se tienen en la actualidad.

Si bien muchos de los componentes disponibles para articular un mercado y comercio electrónico han existido desde hace algún tiempo, es claro que muy poco se ha recabado en las prácticas de programación confiable que éstos pueden tener, y menos en el nivel de pruebas de mal uso o de stress que se pueden haber realizado frente a un uso masivo de los mismos. Las buenas prácticas generalmente utilizadas como las listas de chequeo de OWASP (s.f.), las listas de controles del SANS (s.f.) y algunas recomendaciones del CI-Security (s.f.), son frecuentemente mencionadas cuando se hace referencia a la seguridad en las aplicaciones.

Este escenario de incorporación y puesta en marcha de componentes de tecnología de información en la economía digital de las naciones, establece un patrón emergente de recuperación y motivador de la prosperidad social, el cual se configura como un articulador estratégico de la dinámica empresarial y la punta de lanza de la promoción de innovaciones que construyan nuevas experiencias para los clientes (Flaherty III, Nillesen & Coughlin, 2019).

Para ello, la seguridad y la confianza digital cobran especial relevancia como factores críticos de éxito para consolidar una visión de una economía digital que conecta productos, servicios y clientes (locales e internacionales) con una cadena de distribución que no conoce fronteras. Lo anterior, demanda un liderazgo digital (Kane, Phillips, Copulsky & Andrus, 2019) y una construcción colectiva de capacidades entre los diferentes actores del nuevo ecosistema digital como son los gobiernos, las plataformas internacionales, los sistemas de pagos, las expectativas de los clientes, la oferta novedosa de productos y servicios y la participación de los organismos de vigilancia y control en el contexto digital (Grone, Peladeau & Samad, 2019).

En consecuencia, este artículo presenta un análisis conceptual que define la inseguridad tecnológica como un impuesto progresivo a la dinámica de la economía digital, que puede pasar una amplia factura a las iniciativas innovadoras que se desarrollan en la actualidad, deteriorando la confianza digital necesaria para impulsar las apuestas creativas que se pueden proponer ahora y en el futuro, así como algunas alternativas para promover su elusión en un contexto cada vez más tecnológicamente modificado.

Ciberataques: ¿impuestos a la economía de las naciones?

Cuando entendemos la dinámica de un ciberataque basada en dos dimensiones: el adversario y la amenaza, es viable identificar una amplia gama de posibilidades si dicha dimensión es conocida o desconocida.

Un ciberataque tiene como finalidad última producir mayor incertidumbre en el modelo de seguridad y control de una organización o nación, o expresado de forma más práctica, revelar los puntos ciegos y ocultos en las implementaciones de seguridad que las empresas y las naciones tienen.

Al materializarse un ciberataque en una organización o nación, se dispara una serie de eventos que advierte el nivel de preparación, práctica e inversión para atender una condición adversa en este contexto. Por un lado, se activan los protocolos de atención en el que, tanto el nivel operacional como táctico, intervienen en una primera instancia para coordinar las acciones de verificación y control de la situación, mientras se preparan las comunicaciones requeridas que muestren la diligencia y transparencia de la empresa con sus clientes (Cano, 2016).

Por otra parte, los ejecutivos se notifican de la situación y comienzan a revisar los posibles impactos con los grupos de interés que pueden terminar en sanciones o multas, dependiendo del tipo de información que se pueda haber comprometido.

Es importante anotar que, si la afectación implica infraestructura crítica cibernética nacional la respuesta deberá ser coordinada y efectiva con los diferentes grupos de interés, dados los impactos que el evento puede tener en la gobernabilidad y desarrollo de las funciones del Estado.

Todos los impactos que se pueden ocasionar por cuenta de la explotación de una vulnerabilidad en la infraestructura tecnológica de una organización, o el éxito de una compaña de engaño o desinformación diseñada para desestabilizar empresas de un sector específico, establece un tributo a la dinámica de la economía digital que cobra en la confianza de los clientes dejando una estela de incierto y desencanto de las nuevas iniciati-

vas, como quiera que las personas hoy son más conscientes de la importancia de sus datos y lo que significan para las empresas en el desarrollo de sus modelos de negocios actuales (Hathaway et al., 2015).

Se podría decir que la inseguridad digital es semejante a un impuesto progresivo (López, s.f.), que cuanta mayor incertidumbre e inestabilidad genera, mayor será el deterioro sobre la base de confianza digital disponible. A diferencia de la definición básica de este impuesto, la inseguridad ejerce una amplia presión, no sólo sobre las empresas y naciones, sino sobre los ciudadanos, lo que desincentiva la dinámica económica en el escenario digital y abre una brecha en las relaciones comerciales que puede terminar cobrando en las utilidades esperadas, debido a una falta de condiciones básicas de seguridad y control y a una comprensión exclusiva de la seguridad y ciberseguridad como un fenómeno técnico que está a cargo del área de tecnología de información o de los proveedores de dichas tecnologías.

Ciberataques: ¿tributos que no se pueden eludir o evadir?

Los ciberataques como impuestos progresivos que gravan al final tanto a naciones, como a empresas e individuos, cuyo valor puede ser arbitrario por sus efectos e impactos en los diferentes grupos de interés y que puede provocar desmotivación sobre la inversión en iniciativas digitales (Costa et al., 2005), se configuran como elementos claves y concretos que deben ser revisados de cara a la consolidación de una agenda digital de un país.

Si bien los ciberataques son inevitables, dada la inevitabilidad de la falla, la invisibilidad de vulnerabilidades inherentes en el código de las aplicaciones, así como posibles vulnerabilidades de día cero, las noticias o videos falsos o las acciones de colectivos hacktivistas (digitalmente correctas o incorrectas) (Lizama, 2005), estos representan oportunidades para preparar mejor las empresas y coordinar los esfuerzos para construir una vista común, que aumente la resiliencia de las empresas y las naciones (Cano, 2020).

La dinámica de un ciberataque es crear incierto e inestabilidad para que la organización o nación actúe de forma errática y abra más espacios de acción para el agente agresor. En consecuencia, es necesario crear acciones de preparación y acción colectiva que permitan a las empresas conectarse y diseñar estrategias de protección, colaboración y cooperación que aumenten la resistencia de las organizaciones participantes, creando una estrategia de disuasión creíble y verificable que disuada al tercero de las acciones agrestes que pueda tener planeadas (Sieber & Zamora, 2018).

De tal manera, el impuesto progresivo del ciberataque que inicial-

mente recae de forma evidente y exigente de forma individual tanto para los países, las empresas y los individuos, se hace una carga menos demandante, toda vez que se desarrolla una red extendida de monitorización, inteligencia y acciones coordinadas, que limitan los efectos en los grupos de interés, y muestran el compromiso de la comunidad empresarial frente a la protección del consumidor basado en un ejercicio de simetría, transparencia y reciprocidad construido desde el apetito de riesgo corporativo y los umbrales propios de su operación.

Evadir y eludir los impuestos son dos conductas diferentes y con implicaciones legales distintas. Mientras la evasión de los impuestos es una conducta típica, antijurídica y culpable la cual es llevada a cabo por los sujetos con el fin de evitar total o parcialmente el pago de impuestos, lo que constituye un delito; la elusión es una estrategia legal para librarse de una tasa impositiva, a través de la no realización de las circunstancias que originan la acción tributaria (Brito, 2011).

Si un ciberataque es un impuesto progresivo, la evasión de este impuesto implicaría engañar al adversario en su propio territorio para cambiar la ecuación del incierto en su modelo de riesgo, como una estrategia de defensa activa premeditada que implica comprometer al atacante y sus posibles acciones antes que ocurran, lo que significaría un acción de neutralización del agente agresor de forma anticipada, lo que puede terminar en una acción ilegal de actuación de las empresas o naciones, frente a disposiciones y directrices internacionales frente a actos hostiles de parte de actores multinacionales conocidos o desconocidos.

De otra parte, la elusión se podría concretar a través de una estrategia de defensa pasiva que crea un escenario alterno de monitorización, inteligencia y reconocimiento de patrones para coordinar una acción conjunta con los diferentes actores del ecosistema digital, con el fin de crear una red de respuesta y tratamiento del evento de acuerdo con las condiciones y regulaciones vigentes, en las cuales los centros de atención de incidentes (propios de los sectores productivos y de las empresas) y los comandos conjuntos cibernéticos juegan un papel fundamental para asegurar la integridad de las organizaciones y la protección de sus infraestructuras.

Reflexiones finales

Dentro de las preocupaciones más importantes de los ejecutivos de las empresas a nivel global se encuentran la sobrerregulación, las confrontaciones comerciales internacionales, el entorno incierto de crecimiento, las ciberamanazas y la incertidumbre política (PwC, 2020), tensiones que afectan las reflexiones y decisiones de las juntas directivas en las organizaciones, de cara al reto de una transformación

digital apresurada que puede marcar una diferencia positiva o menos afortunada para sus planes de negocio.

Las ciberamenazas y la materialización de los ciberataques ponen sobre la mesa de trabajo de países, empresas y personas inquietudes relevantes que afectan la economía global, las utilidades y los derechos fundamentales como un sistema socio-técnico que se articula con infraestructura, aplicaciones y servicios que se despliegan en un escenario digitalmente modificado (Li & Horkoff, 2014). En este sentido, crean un sistema de tracción que afecta la dinámica de la economía digital, desarrollando un impuesto progresivo que grava la confianza digital de los consumidores a nivel global.

Por lo tanto, mientras no se comprenda que el riesgo cibernético es un nuevo tipo de riesgo que emerge de una dinámica aumentada de la densidad digital (Cano, 2019), de una necesidad de transformación en la manera que se han las cosas y cómo un habilitador de la prosperidad de una nación, que implica una acción colectiva para su tratamiento, estaremos tributando de forma progresiva en cada uno de los grupos de interés sobre los posibles beneficios económicos y sociales de las iniciativas digitales, generando brechas de inequidad que terminan afectando la productividad y el bienestar de países, empresas y personas.

La materialización de un ciberataque es una situación que rompe con las certezas que se tienen en los modelos tradicionales de seguridad y control, lo que crea inestabilidad e incierto en las actuaciones de las naciones y empresas. Por tanto, es necesario reconstruir los supuestos de base del entendimiento de la dinámica empresarial para pasar de una postura de "riesgo cero" a una política de umbrales de operación, donde se reconoce la falla como parte inherente de la práctica empresarial y como base de una cultura de aprendizaje que hace más resistente a la empresa y la nación frente a estos eventos (Dupont, 2019).

De esta manera, los impuestos progresivos que imponen la materialización de los ciberataques podrán responder a una estrategia de elusión debidamente planeada y elaborada de forma conjunta con los diferentes actores de la sociedad, de tal manera que los agresores perciban una acción coordinada y unificada, que entiende el incierto como parte natural del entorno de trabajo de naciones, empresas y personas, y donde los eventos inesperados y acciones agresivas constituyen un punto de inflexión donde es posible mantener las operaciones, invertir y capitalizar los aprendizajes, y salir fortalecidos a pesar del éxito de los adversarios.

Así las cosas, si la ciberseguridad, al igual que el aprendizaje, no es un

deporte de espectadores sino que exige la participación de todos los grupos de interés (Iny, 2018), y un ciberataque, es una forma inesperada para sacar a las organizaciones, países y personas fuera de la zona cómoda o conocida, la economía digital debe ser el escenario donde se configuren las condiciones necesarias y suficientes para crear una zona de balance dinámico y de estabilidad digital que permita, no sólo capitalizar nuevas propuestas de negocios digitales, sino asegurar una vista conjunta que diseñe, implemente y limite la base impositiva que los diferentes adversarios conocidos o desconocidos, actuales o emergentes quieran concretar e imponer sobre todos los actores de la dinámica social.

Referencias

Brito, J. (2011). Teoría de los ingresos públicos. *Materiales de economía*. Departamento de Análisis Económico Aplicado. Universidad de Las Palmas de Gran Canaria. https://www.personales.ulpgc.es/jbrito.daea/9.%20TeoriaIngresosPublicos.PDF

Cano, J. (2016). Ciberataques. La inestabilidad de lo que hemos aprendido en seguridad y control. *ISACA Journal*. 5. https://www.isaca.org/Journal/archives/2016/volume-5/Pages/cyberattacks-the-instability-of-security-and-control-knowledge-spanish.aspx

Cano, J. (2019). Ciberriesgo. Aprendizaje de un riesgo sistémico, emergente y disruptivo. *Revista SISTEMAS*. Asociación Colombiana de Ingenieros de Sistemas. 63-73. https://doi.org/10.29236/sistemas.n151a5

Cano, J. (2020). ¿Por qué los ciberataques son inevitables?: Prácticas y capacidades claves de la ciberseguridad empresarial. En Gauthier-Umaña V., Méndez-Romero R., & Suárez D. (Eds.), *Voces diversas y disruptivas en tiempos de Revolución 4.0* (pp. 223-248). Bogotá, D. C.: Editorial Universidad del Rosario. doi:10.2307/j.ctv123x566.14

CISecurity (s.f). Application software security. *CIS Controls*. CIS Control 18. https://www.cisecurity.org/controls/application-software-security/

Cooray, M. & Duus, R. (2020). DVC Framework: Accelerating Digital Value Creation. *European Business Review*. https://www.europeanbusinessreview.com/dvc-framework-accelerating-digital-value-creation/

Costa et al. (2005). *Teoría básica de los Impuestos: un enfoque económico*. España: Ed. Civitas

Dupont, B. (2019). The Cyber-Resilience of Financial Institutions: A preliminary working paper on significance and applicability of digital resilience. *Global Risk Institute*. https://globalriskinstitute.org/publications/the-cyber-resilience-of-financial-institutions-a-preliminary-working-paper-on-significance-and-applicability-of-digital-resilience/

Flaherty III, T., Nillesen, P. & Coughlin, M. (2019). Power strategies. *Strategy+Business*. https://www.strategy-business.com/article/Power-strategies

Grone, F., Peladeau, P. & Samad, R. (2019). Tomorrow's Data Heroes. *Strategy+Business*. https://www.strategy-business.com/article/Tomorrows-Data-Heroes

Hathaway, M. et al. (2015). Índice de preparación cibernética 2.0. Un plan para la preparación cibernética: una línea de base y un índice. *Potomac Institute for Policy Studies*. https://www.belfercenter.org/sites/default/files/files/publication/cyber-readiness-2.0-spanish-v2.pdf

Iny, D. (2018). *Leverage learning. How the disruption of education helps lifelong learners and experts with something to teach*. USA: Ideapress Publishing.

Kane, G., Phillips, A., Copulsky, J. & Andrus, G. (2019). How Digital Leadership Is(n't) Different. *Sloan Management Review*. Spring. https://sloanreview.mit.edu/article/how-digital-leadership-isnt-different/

Li, T. & Horkoff, J. (2014) Dealing with Security Requirements for Socio-Technical Systems: A Holistic Approach. En Jarke M. et al. (eds) *Advanced Information Systems Engineering*. CAiSE 2014. Lecture Notes in Computer Science, vol 8484. Springer. https://doi.org/10.1007/978-3-319-07881-6_20

Lizama, J. (2005). Hackers en el contexto de la sociedad de la información. Facultad de Ciencias Políticas y Sociales. *Tesis doctoral*. http://132.248.9.195/pd2005/0601439/0601439.pdf

López, D. (s.f.) Impuesto progresivo. Economipedia. https://economipedia.com/definiciones/impuesto-progresivo.html

OWASP (s.f.). OWASP top ten. *OWASP foundation*. https://owasp.org/www-project-top-ten/

PwC (2020). Navigating the rising tide of uncertainty. *23rd Annual Global CEO Survey*. https://www.pwc.com/ceosurvey

SANS (s.f). Web applications. *SCORE: Checklists & Step-by-Step Guides*. https://www.sans.org/score/checklists/web-applications

Sieber, S. & Zamora, J. (2018). The Cybersecurity Challenge in a High Digital Density World. *European Business Review*. November. https://www.europeanbusinessreview.com/the-cybersecurity-challenge-in-a-high-digital-density-world/

Jeimy J. Cano M., Ph.D, CFE, CICA. *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 en Business Administration por Newport University, CA. USA. y Ph.D en Educación por la Universidad Santo Tomás. Profesional certificado como Certified Fraud Examiner (CFE), por la Association of Certified Fraud Examiners y Certified Internal Control Auditor (CICA) por The Institute of Internal Controls. Profesor Distinguido de la Facultad de Derecho, Universidad de los Andes. Es director de la revista Sistemas de la Asociación Colombiana de Ingenieros de Sistemas –ACIS–.*

Ciencias satelitales e inclusión social

DOI: 10.29236/sistemas.n157a7

Satélites sociales e Ingenieros sin fronteras hacia la inclusión social.

Manuel Dávila Sguerra

La Unión Europea define la inclusión social como un "proceso que asegura que aquellas personas que están en riesgo de pobreza y exclusión social tengan las oportunidades y recursos necesarios para participar completamente en la vida económica, social y cultural disfrutando un nivel de vida y bienestar que se considere normal en la sociedad en la que ellos viven". Hace énfasis en el derecho de las personas de "tener una vida asociada siendo un miembro de una comunidad" (Andalucía solidaria, 2020).

El tema satelital aparece porque a través de los satélites es posible estudiar el estado de la tierra y dirigir los resultados de estos análisis a los agricultores y, en general, a las comunidades relegadas para controlar sus propios territorios.

Ingeniería humanitaria

La Ingeniería Humanitaria se está convirtiendo en un *"eEstado del arte"* que, de acuerdo con información conocida de la Universidad Sergio Arboleda (U Sergio Arboleda, 2020), la Universidad Nacional