Fundamentos de ciberseguridad:

reflexiones convergentes para construir un entorno digital menos inseguro

Jeimy J. Cano, Ph.D, CFE
Miembro investigador del Grupo de Estudios en Comercio Electrónico[1]

1 El autor agradece los valiosos y generosos comentarios de profesionales distinguidos como Manuel Dávila, Pedro Hecht, Rodrigo López Lio, Gabriela Saucedo y Diego A. Zuluaga, quienes permitieron afinar las ideas y reflexiones de este artículo.

fot: http://www.diariodigitalcolombiano.com/colombia-entre-los-mejores-del-mundo-en-ciberseguridad/

Resumen

El ciberespacio y sus relaciones emergentes plantean nuevos retos tanto para los individuos y las organizaciones como para las naciones. Uno de ellos, relacionado con la seguridad y control en un mundo globalizado y automatizado, requiere una aproximación convergente, que permita entender la dinámica e impactos de la protección de los sistemas de información empresariales y las realidades de los sistemas de control industrial, que operan infraestructura clave de una nación. En este sentido, este artículo plantea una propuesta conjunta de seguridad y control, donde se define la ciberseguridad como un instrumento de política de Estado, que se materializa en una práctica para evitar que el mundo afecte el sistema y de igual forma evitar que el sistema afecte al mundo.

Introducción

La seguridad de la información es siempre un producto en desarrollo, un ejercicio de aseguramiento y descubrimiento permanente que no admite posiciones incontrovertibles o sesgos de visiones particulares. Es una disciplina que está en constante movimiento y renovación como premisa fundamental para mantener el espacio conocido de riesgo residual aceptable y tolerable por una persona u Organización.

En este sentido, cada vez más, las decisiones relacionadas con protección de la información tienen impactos significativos en aspectos claves de la vida de las personas. Casos particulares se observan en aquellos puntos donde las tecnologías de información convergen con los sistemas de control, los cuales generalmente terminan teniendo a cargo sistemas de transporte de energía, monitoreo de plantas, operación de dispositivos biomédicos, entre otros, que se integran y afectan aspectos claves de la vida humana.

Así las cosas, se abre un camino convergente entre dos conceptos ampliamente utilizados en el dominio de la seguridad y control como son *safety y security.* De acuerdo con Axelrod (2013), se entiende por *safety* – que el sistema no debe dañar al mundo – y por *security* – que el mundo no debe dañar el sistema. Ahora bien, si el sistema es susceptible a las dos distinciones estamos en presencia de una infraestructura crítica donde el sistema puede llegar a "dañar el mundo" y "el mundo puede dañarlo" (JCM-14: 1).

En consecuencia, cuando trasladamos estas dos distinciones a la esfera de la seguridad de la información y de la ciberseguridad, comenzamos a vislumbrar los enfoques complementarios que se deben asumir para avanzar en nuevas prácticas de aseguramiento en un contexto extendido de la realidad del flujo de la información que afecta el mundo exterior y puede comprometer la vida humana.

> "...en el pasado, eran unos pocos los que tenían el control de los contenidos que se subían a la infraestructura; hoy el proceso de apertura y democratización que ha tenido el ciberespacio, permite que cualquier persona que tenga acceso a este mundo digital, tenga la capacidad de crear sus propios contenidos y propagarlos de la forma que mejor le parezca".

Mientras las prácticas de seguridad de la información tradicionales, se concentran en que "el mundo no dañe el sistema", procurando una serie de acciones y actividades que incrementen la resistencia del sistema a los ataques, las nuevas estrategias de ciberseguridad, deben sintonizar las anteriores para evitar que el sistema "pueda dañar el mundo", esto es, entender la misión que tiene el sistema en el mundo y sus impactos, para así desarrollar un enfoque agregado de protección que evite dañar la realidad exterior y asegurar la resistencia del sistema frente a ataques del exterior.

Siguiendo las reflexiones de Clark y Knake (2010), el ciberespacio es una realidad emergente que se

Foto: http://www.pandasecurity.com/spain/mediacenter/panda-security/ejemplos-ciberdelincuencia-segundo-trimestre-2013/

compone de cuatro elementos fundamentales: *contexto físico, fundamentos lógicos, contenidos y actores.* Cada uno de ellos interactuando entre sí, le dan vida a un ente de construcción colectiva que vincula el mundo real con la realidad digital del flujo de información, donde se construyen y reinventan las relaciones entre los diferentes actores.

Por su parte en el pasado, eran unos pocos los que tenían el control de los contenidos que se subían a la infraestructura; hoy el proceso de apertura y democratización que ha tenido el ciberespacio, permite que cualquier persona que tenga acceso a este mundo digital, tenga la capacidad de crear sus propios contenidos y propagarlos de la forma que mejor le parezca.

En este escenario, el ciberespacio según Choucri (2012), es una plataforma de interacción humana, soportada en una realidad tecnológica que ofrece las siguientes características: es atemporal e instantáneo; ubicuo; está en todas partes; es permeable; traspasa todas las fronteras; es fluido; está en revolución y cambio permanente; es participativo y universal; de contribución popular; con múltiples identidades; procura el anonimato; es autorregulado y finalmente, busca la neutralidad tecnológica.

En consecuencia, el ciberespacio establece un reto conceptual y práctico tanto para la sociedad, como para las diferentes disciplinas científicas, pues sus múltiples aproximaciones y variables, motivan diversas reflexiones que crean visiones y tendencias aprobadas por algunos y controvertidas por otros (Clark; Berson y Lin 2014, Choucri, 2012).

Así, una política de ciberseguridad es un instrumento que desarrollan las naciones para comunicar y manifestar aquellos aspectos que un Estado desea proteger en el ciberespacio. Es una declaración que materializa la postura de un gobierno para vincular de manera decidida al ciudadano, sus derechos y deberes ahora en un escenario de la realidad extendida de la sociedad, donde la información instantánea, la movilidad y las redes sociales son la norma de su operación.

Buscando respuestas para la ciberseguridad

Siguiendo las reflexiones de Axelrod (2013, pág. 117) sobre *safety* y *security* se hace necesario distinguir entre los sistemas de información críticos y sistemas de control críticos. Para ello, propone distinguirlos por las consecuencias que puede traer su mal funcionamiento, uso inadecuado o falla. Mientras una falla en un sistema de información crítico puede llegar a tener impactos económicos, sociales y legales, en los sistemas de control los efectos pueden ocasionar daños físicos y/o daños al ambiente.

En este tenor, podríamos indicar que la ciberseguridad, es el conjunto de prácticas de seguridad y control aplicadas sobre sistemas de información y/o control que operan en el ciberespacio, con el fin de hacerlos más resistentes a los ataques (security), limitando los impactos adversos en el mundo exterior producto de su malfuncionamiento, uso inadecuado o falla (safety).

Habida cuenta de lo anterior, se comprenden mejor las preocupaciones de los gobiernos y organismos multilaterales sobre los eventos recientes que afectan la operación de plantas de energía, refinerías, aeropuertos, dispositivos biomédicos, los sistemas de defensa, sistemas bursátiles, entre otros, que buscan no solamente atacar el sistema, sino producir un daño en el mundo real, que genere confusión y zozobra frente a las posibilidades que se manifiestan en la interrelación entre el ciberespacio y los sistemas de control (Gonsalves, Kepes, Riley, 2014).

Reflexiones finales

Los ciberataques cada vez serán más comunes y sus impactos comenzarán a inquietar a las empresas y gobiernos, pues no solamente habrá cicatrices en sistemas o tecnologías particulares, sino que sus efectos alcanzarán sectores claves de un país, afectando la población civil y el normal desarrollo de sus actividades, como ha ocurrido en el pasado.

La complejidad tecnológica, la rapidez de la evolución tecnológica, la falta de madurez de la industria de TI, la alta interconectividad de las "cosas"

> ... una política de ciberseguridad es un instrumento que desarrollan las naciones para comunicar y manifestar aquellos aspectos que un Estado desea proteger en el ciberespacio".

y la visibilidad de los elementos de la operación del mundo OT (Candau 2013), aumentan la posibilidad para que los atacantes descubran en el laberinto de direcciones IP, aquellos sitios neurálgicos de las operaciones de una empresa o país, y provocar una crisis que ponga en tela de juicio la gobernabilidad de un Estado.

La ciberseguridad como la intersección entre política y tecnología, así como prácticas de seguridad y control convergentes de los mundos *safety* y *security*, plantean nuevos retos y desafíos para los ejecutivos de seguridad de la información, los

Foto: http://www.acfcs.org/convenience-drives-technology-and-cybersecurity-risks-says-karen-lissy-financial-cyber-crime-expert/

"... la ciberseguridad, es el conjunto de prácticas de seguridad y control aplicadas sobre sistemas de información y/o control que operan en el ciberespacio, con el fin de hacerlos más resistentes a los ataques (security), limitando los impactos adversos en el mundo exterior producto de su malfuncionamiento, uso inadecuado o falla (safety)".

presidentes de empresa y los gobernantes de las naciones, toda vez que el tejido social, ahora intercomunicado por una infraestructura tecnológica, se hace más susceptible a fallas o malos usos, cuyos impactos en número de víctimas potenciales, impactos económicos y afectación de la confianza del público, estamos empezando a conocer y caracterizar.

Estamos ante un escenario incierto, que toma a personas, empresas y naciones sin la preparación adecuada, como quiera que hasta ahora la mirada sobre la seguridad de la información se habían concentrado hacia el interior y como problema local, descuidando de igual forma la evolución y visibilidad de los sistemas OT, propios de la vista de aquellos sistemas que no deben dañar el mundo.

Si bien este artículo no pretendió agotar las reflexiones sobre ciberseguridad, sí propuso un punto de reflexión conceptual para motivar la generación de nuevas propuestas de construcción de un concepto, que no puede ser tratado como una extensión de las prácticas tradicionales de seguridad y control, sino como un ejercicio donde política y tecnología se hacen convergentes para reinventar la noción del Estado-nación más allá de las fronteras conocidas e incorporar al ciberespacio como el nuevo contorno de la realidad social, tan real y vibrante como la soberanía de un país y su Estado social y democrático de Derecho.

Foto: http://www.cios.com/i/cybersecurity-spending-more-proactive-than-reactive/

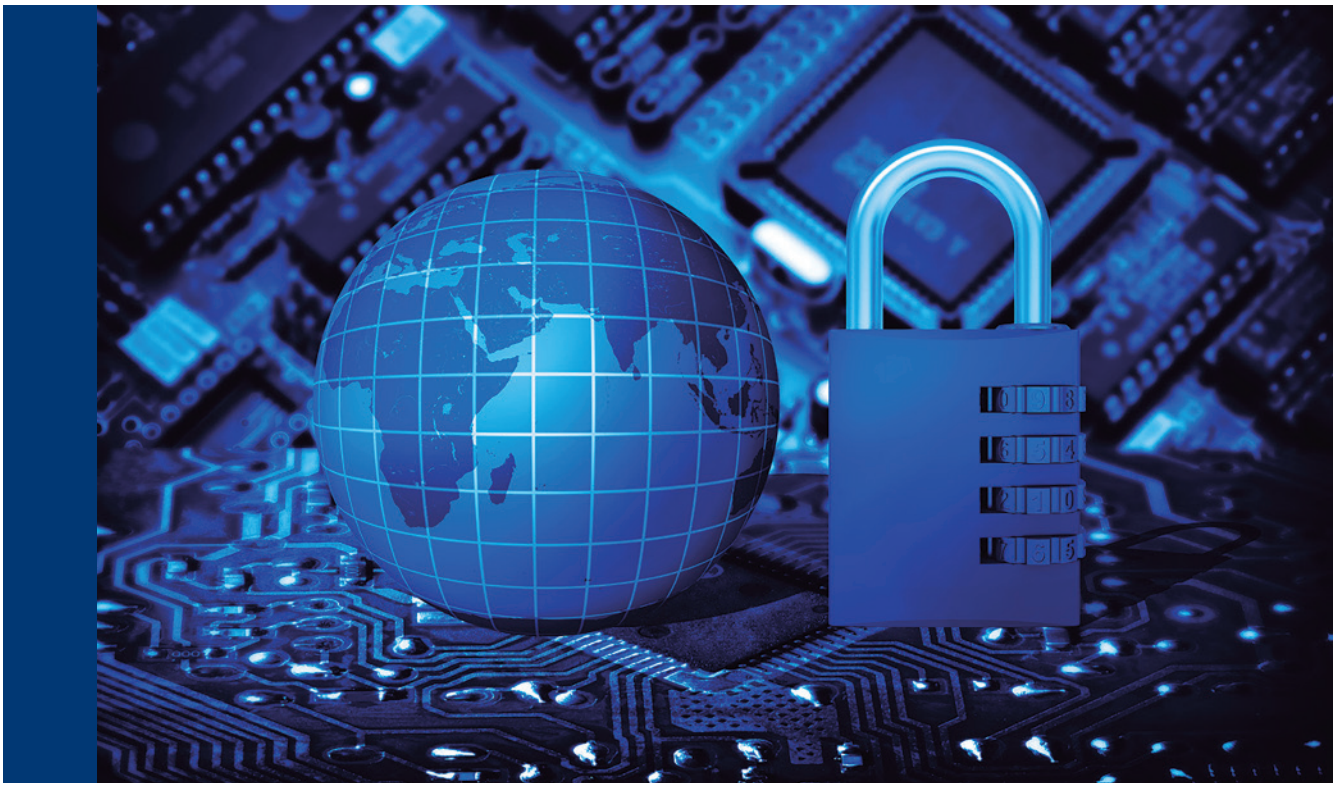

Foto: http://ec.europa.eu/digital-agenda/en/cybersecurity

Referencias

» *Fuentes académicas*

➢ AXELROD, C. W. (2013) Engineering safe and secure software systems. Ed. Artech House.

➢ CANDAU, J. (2013) Prioridades nacionales en ciberseguridad. En SEGURA, A. y GORDO, F.

➢ CHOUCRI, N. (2012) Cyberpolitics in international relations. MIT Press.

➢ CLARK, D., BERSON, T., y LIN, H. (Editors) (2014) At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues. National Research Council. National Academies Press.

➢ CLARK, R. y KNAKE, R. (2010) Cyber war: The next threat to National Security and what to do about it. HarperCollins.

» *Fuentes electrónicas*

➢ GONSALVES, A. (2014) Airport Breach a Sign for IT Industry to Think Security, Not Money. Disponible en: http://www.cio.com/article/2448928/it-strategy/airport-breach-a-sign-forit-industry-to-think-security--not-money.html (Consultado: 1-07-2014)

➢ KEPES, B. (2014) Data Security And What Keeps CISOs Up At Night. Disponible en: http://www.forbes.com/sites/benkepes/2014/06/27/data-security-and-what-keeps-cisosup-at-night/?ss=cio-network (Consultado: 1-07-2014)

➢ JCM-14 All rights reserved Página 12 de 13

CURRÍCULUM

Jeimy J. Cano: Ph.D, CFE; Ph.D in Business Administration de Newport (University, CA –USA). Certificate in Management and Leadership (MIT Sloan School of Management, MA-USA, Profesional); Certified Fraud Examiner (CFE) por la Association of Certified Fraud Examiners y Cobit. Ingeniero y Magíster en Ingeniería de Sistemas y Computación (Universidad de los Andes). Especialista en Derecho Disciplinario por la Universidad Miembro investigador del Grupo de Estudios en Comercio Electrónico, Telecomunicaciones e Informática (GECTI) de la Facultad de Derecho (Universidad de los Andes).