

Seguridad de la información y ciberseguridad empresarial

DOI: 10.29236/sistemas.n155a1



Jeimy J. Cano M.

De las buenas prácticas al desarrollo de capacidades. Los nuevos escenarios que propone la convergencia tecnológica y de disciplinas científicas abren oportunidades y retos inéditos, así como amenazas emergentes.

Revisando las reflexiones en el número 115 de la Revista “SISTEMAS”, publicado en 2010 sobre el futuro de la seguridad de la información, se afirmaba que: “*las enseñanzas de la inseguridad de los últimos 10 años podríamos resumirlas en una exigente necesidad de interconexión permanente, acceso a la*

información ágil e instantánea y sobremanera, interacción constante y sin restricciones” (Cano, 2010).

Esta afirmación muestra que, durante la primera década del nuevo milenio, la conectividad creó un escenario digital de interacción permanente, en el que se configuró un

“halo” de confianza en la tecnología de información y comunicaciones para un aumento en el flujo de datos que privilegió la eficiencia de las operaciones en las empresas. En este sentido, y muchas veces sin notarlo, se fueron configurando fallas y vulnerabilidades, perfeccionando las estrategias de los adversarios con ataques novedosos.

Lo que ocurrió durante la segunda década del milenio coincide con los análisis planteados en el número 115 de nuestra revista. La convergencia de la seguridad de la información con la seguridad física y electrónica, la tercerización de las áreas de tecnología de información y la desobediencia de los usuarios se convirtieron en la base de los retos para los profesionales de la seguridad de la información los cuales, cruzados con las cambiantes exigencias del negocio y la dinámica de los mercados, configuraron un caldo de cultivo sazonado para la propagación de la inseguridad en cada uno sus actores (Cano, 2010).

La perspectiva para los próximos diez años (2020-2030) sugiere un escenario diferente y con experiencias aumentadas para los clientes de las empresas. Los ecosistemas digitales, la realidad aumentada, las cadenas de bloques, la computación en el borde y el advenimiento de los sistemas ciberfísicos, desplegados en las diferentes industrias y sectores productivos, serán el nuevo contexto para que los adversarios tomen posiciones estra-

tégicas y desarrollen nuevas propuestas agresivas que tensionen los renovados modelos de seguridad y control de las compañías (Cano, 2020).

En este contexto, la sensación de que “pensábamos que conocíamos los riesgos”, da lugar a una nueva lectura de la realidad, en un ambiente cibernéticamente aumentado, con situaciones inéditas para las organizaciones y cuyo tratamiento no responde ni a las buenas prácticas ni a los estándares vigentes, sino al desarrollo de capacidades para defender y anticipar escenarios asimétricos.

Es por esto que la revista “SISTEMAS”, de la Asociación Colombiana de Ingenieros de Sistemas –ACIS–, ha decidido revisar, explorar y analizar en prospectiva la dinámica de la seguridad/ciberseguridad en los próximos diez años. Con ese objetivo, fueron convocados profesionales de distintas disciplinas, quienes desde su área de experiencia proponen reflexiones para seguirle la pista al desarrollo de la protección de los conocidos activos de información y los nuevos activos digitales, desde las lecciones aprendidas, los negocios y retos actuales, así como las tendencias futuras que desde hoy se avizoran en el horizonte.

El ingeniero Armando Carvajal Rodríguez, columnista invitado, establece desde su práctica de consultoría un marco base para reflexio-

nar sobre la seguridad de la información y la evolución de la inseguridad, como un reto clave en la gestión de riesgos y como fundamento para advertir iniciativas de ataque y responder a los hechos que podrían desestabilizar empresas y naciones. En esa dirección presenta el artículo “Reflexiones sobre la seguridad de la información en la economía 5.0”.

El entrevistado en este número de la revista es José Eduardo Campos, especialista en ciberseguridad, con más de 25 años de experiencia, consultor y director de proyectos innovadores de desarrollo empresarial en los Estados Unidos, con enfoque en mercados emergentes en América Latina, Sudeste Asiático e India.

Por su parte, el ingeniero Andrés Almanza Junco presenta el análisis de los resultados de la versión número veinte de la encuesta nacional de seguridad de la información, realizada cada año por ACIS, estudio que revela las tendencias más representativas de las empresas colombianas en los temas de protección de la información y la evolución del líder digital de seguridad, así como sus respectivos contrastes con la realidad internacional. En esta oportunidad, se observan dos décadas de la evolución de las prácticas de seguridad y control en las empresas y en el país.

El foro contempla la validación y prospectiva de la seguridad y con-

trol, en la opinión de los mismos participantes en el foro del año 2010. Los ingenieros Juan Camilo Reyes, Javier Díaz, Evans, Andrés Almanza Junco y el abogado Rafael Gamboa Bernate revisaron sus planteamientos de esa época, en el marco de los últimos 10 años, para documentar su visión a 2030 para los negocios. Ellos advierten sobre la necesidad de reinventar las prácticas de seguridad de la información, además de avanzar en una perspectiva interdisciplinaria, orientada a que los profesionales y ejecutivos de seguridad y control puedan enfrentar un escenario cada vez más disruptivo, inestable e hiperconectado, con una mayor exigencia de anticipación, más que de prevención.

Así mismo, nuestros lectores dispondrán de dos artículos sobre el uso de la movilidad como estrategia de formación en seguridad de la información y las lecciones aprendidas en seguridad y control durante los últimos diez años. Un primer documento de autoría del ingeniero Julio Poveda Gómez, se ocupa de analizar las vías para articular las estrategias de “aprendizaje móvil”, a través de una aplicación para enseñar conceptos de seguridad informática.

El segundo artículo, escrito por este servidor, aborda las lecciones aprendidas en la última década en seguridad de la información, así como los retos emergentes para la seguridad/ciberseguridad. Allí se es-

tablecen cinco temáticas relevantes (*la computación la nube, la computación móvil, la convergencia tecnológica, las redes sociales y la asimetría de los ciberconflictos*), que sustentan las bases para asumir los retos en el marco de las empresas digitales y tecnológicamente modificadas.

La totalidad de este contenido muestra un panorama actual y prospectivo de las prácticas y desafíos de la seguridad/ciberseguridad, como una excusa académica y práctica para superar las certezas propias de los estándares y prácticas existentes. Los diferentes temas invitan a todos los profesionales en las diferentes áreas, a explorar las nuevas realidades de la

protección de los activos de información y de los nuevos activos digitales, sin perjuicio de la transformación de los retos e inestabilidades políticas, económicas, sociales, tecnológicas, legales y ecológicas vigentes y futuras.

Referencias

- Cano, J. (2010) Seguridad de la información: ¿qué hemos aprendido y para dónde vamos? *Revista SISTEMAS*. Asociación Colombiana de Ingenieros de Sistemas (ACIS). 115. 4-1.
- Cano, J. (2020) Retos de seguridad/ciberseguridad en el 2030. Reflexión sobre un ejercicio prospectivo incompleto. *Revista SISTEMAS*. Asociación Colombiana de Ingenieros de Sistemas (ACIS). No. 154. 68-79. Doi: 10.29236/sistemas.n154a7. 

Jeimy J. Cano M., Ph.D, CFE, CICA. *Profesor distinguido de la Facultad de Derecho. Universidad de los Andes. 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 Business Administration en Newport University, CA. USA. y Ph.D en Educación, 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. Es director de la revista Sistemas de la Asociación Colombiana de Ingenieros de Sistemas–ACIS–.*