Cuarta revolución industrial: anticipo de un nuevo desarrollo de la humanidad

El evidente impacto de la cuarta revolución industrial en la sociedad completa, pone de manifiesto desafíos sociales, económicos, políticos y tecnológicos. En este sentido, los nuevos productos y servicios digitalmente modificados exigen un análisis de los retos y paradigmas de la seguridad y el control, como fundamento de la confianza requerida para que se haga realidad su promesa de valor.

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

No existe un espacio en el que la cuarta revolución industrial deje de ser protagonista. Figura en primera fila en mesas de debate, consejos académicos, conferencias, charlas informales y en los medios de comunicación especializados y los de interés general.

Esta nueva realidad digital y tecnológicamente modificada establece un cambio de paradigma en la sociedad actual que entra en tensión con las estrategias de negocio conocidas, con el fin de cambiar una percepción del cliente y crear una experiencia dife-

rente en el desarrollo de las actividades propias de las personas y sus retos.

Por esa razón, la revista Sistemas dedicó de lleno las páginas de su edición número 143, a hilvanar y deshilvanar los retos y paradigmas que la seguridad y el control afrontan en el marco de la cuarta revolución industrial. Un ejercicio que confronta los saberes previos de la práctica de seguridad de la información frente a las exigencias de los negocios, que demandan asumir riesgos retadores y calculados.

Cada una de las secciones se ocupa de una mirada al respecto. Con una visión holística, el ingeniero Eduardo Carozo Blumsztein aborda los beneficios, impactos y desafíos tecnológicos, como columnista invitado. El ingeniero Carozo, profundiza en las bondades de esta nueva revolución, con una mirada reposada sobre las condiciones de seguridad y control requeridas.

Por su parte, Rebecca Herold, reconocida y premiada consultora internacional, nos concedió una amplia entrevista, donde nos comparte sus puntos de vista sobre los asuntos más neurálgicos de la seguridad de la información y la protección de los datos. Desde su vista global, nos ilustra las exigencias y grandes desafíos que implica un flujo de datos continuo e inesperados entre los "objetos digitalmente modificados".

En la mesa de debate para la sección "Cara y Sello", nos preguntamos si la seguridad y el control son viables, también en el marco de la cuarta revolución industrial. Expertos analistas –por cierto de muy variados perfiles-, asistieron al encuentro para analizar aspectos tales como los riesgos, las amenazas, los cambios en los estándares, las prácticas de seguridad y de control, los cambios normativos sobre el tratamiento de la información, las empresas con infraestructura crítica, el analista de seguridad, además de las habilidades, competencias y conocimientos de los nuevos profesionales, entre los más destacados asuntos.

La encuesta nacional de seguridad informática 2017, capítulo Colombia, realizada por esta Asociación, a través de Internet, contó con la participación de 128 encuestados, quienes con sus respuestas permiten conocer la realidad del país. Este estudio cumple con varios propósitos. En primer lugar, muestra el panorama de las organizaciones colombianas frente a la seguridad de la información y/o ciberseguridad, y su respuesta a las demandas del entorno actual. En segunda instancia, es un instrumento referente para Colombia y Latinoamérica, en la medida en que llama la atención de todos los sectores interesados en los temas relacionados con la seguridad de la información.

El primero de los artículos, plantea un ejercicio de construcción conjunta en ciberseguridad y seguridad de la información que se denomina "*Juegos de guerra*". 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 definidas.

Y para finalizar, el segundo artículo denominado "*IoT: interconexión digital, un reto mayor de seguridad*", describe el panorama de los cambios que los nuevos desarrollos tecnológicos introducen cuando las "cosas" son modificadas tecnológicamente. El autor establece un escenario de desafíos de seguridad y control que son relevantes para todos aquellos que quieren comprender las nuevas realidades emergentes propias del "internet de las cosas".

En resumen, esta edición de la revista nos permite explorar aspectos novedosos de una realidad que pronto nos abordará con todos sus desarrollos, por lo cual se hace necesario iniciar las reflexiones sobre las implicaciones de la seguridad y control como fundamento de la actualización de las prácticas de protección que la sociedad deberá asumir, para concretar las ventajas y logros que se esperan de esta nueva era, donde lo digital deberá converger con lo social, como anticipo de la transformación de las nuevas competencias cognitivas que lleven a un nuevo nivel de desarrollo a la humanidad.

Referencia

Cano, J. (2017) Juegos de guerra. Un ejercicio de construcción conjunta en ciberseguridad y seguridad de la información. *Revista Sistemas*. No. 143. Abril-Junio.

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.*