Seguridad y control ¿son viables?

La llamada cuarta revolución industrial trae 'bajo el brazo' tantos cambios, que el ser humano será otro, en su cotidianidad, en sus relaciones y hasta en su interior. Por supuesto, su entorno también será distinto y en ese ambiente que lo rodea la seguridad es protagonista. Asuntos que enmarcaron el Cara y Sello de esta edición.

Sara Gallardo M.

El salto de la máquina de vapor a los robots integrados en sistemas ciberfísicos, capaces de interactuar con seres humanos, es incalculable. Tales desarrollos tecnológicos han dado lugar a lo que los economistas optaron por definir como cuarta revolución industrial, un momento de la humanidad que quedará grabado en la historia universal, con un sello único.

Ese hecho sin precedentes, basado en Internet de las Cosas, impresión 3D, inteligencia artificial y nanotecnología producirá un hombre distinto, en un entorno también transformado por estas y otras tecnologías de la información y las comunicaciones (TIC). Y la seguridad, en todas sus acepciones, juega un papel muy importante.

En la mirada a ese panorama, hay de todo. Muchos pronostican beneficios para la sociedad y las economías, mientras otros más escépticos, lo contemplan con sigilo. “La hiper-conec-

tividad y las redes sociales nos están dividiendo en vez de unirnos. Existe más presión por actuar rápido, por lo que la democracia representativa se debilita y la toma de decisiones es cortoplacista. El 2016 nos mostró que las personas confunden opiniones con hechos, y rápidamente aceptan evidencia que confirma nociones preconcebidas o convicciones prejuiciosas", en opinión de Javier Arreola[1].

Este y otros asuntos como riesgos, amenazas, cambios en los estándares, prácticas de seguridad y control, cambios normativos sobre el tratamiento de la información, empresas con infraestructura crítica, el analista de seguridad, habilidades, competencias y conocimientos de los nuevos profesionales y la preparación de la Academia, fueron programados para el debate al que asistieron: María Del Pilar Sáenz Rodríguez, coordinadora de Proyectos de la Fundación Karisma; Jaime Eduardo Santos Mera, vicepresidente Legal de Gobierno Mercantil, de Colpatria S.A.; Juan Mario Posada Daza, gerente de Asesoría y Líder de servicios de Ciberseguridad en EY (antes Ernst & Young); Marcela García Caballero, head PR y Spokersperson de Rappi; Andrés Aguilera Castillo, profesor asociado, investigador de la Universidad EAN y Mauricio Guerrero Cabarcas, profesor asociado, investigador de la Universidad EAN.

"De cara al mundo digitalmente modificado -tal y como lo define en forma muy acertada el profesor Michael Porter-, los temas de seguridad adquieren una dimensión muy distinta y dirigen el pensamiento hacia nuevos horizontes que nos van a sorprender. De ahí que muchas consultoras adviertan sobre los 18 billones de dispositivos conectados que existirán en el futuro próximo y los riesgos a los que están expuestas todas las industrias", fue el preámbulo del director de la revista y

1 Javier Arreola, Executive, Investment Banking, GF Inbursa. *5 inquietudes que dejó el Foro de Davos*. 10 Febrero 2017. https://www.weforum.org/es/agenda/2017/02/5-inquietudes-que-dejo-el-foro-de-davos. Recuperado Junio 5 de 2017.


Pilar Sáenz


Marcela García


Jaime Eduardo Santos


Juan Mario Posada


Andrés Aguilera


Mauricio Guerrero

editor técnico en esta edición, Jeimy J. Cano M., quien, dio inicio al debate con la primera pregunta:

¿Cuáles son los nuevos riesgos y amenazas que pueden surgir como consecuencia de la cuarta revolución industrial?

Marcela García C.
Head PR y Spokersperson
Rappi
Que la seguridad vaya más despacio que la misma revolución, es decir, que no alcancemos a llevarle el ritmo y que, por ende, se abran unas brechas importantes y bastante delicadas que promuevan los ataques que estamos viendo hoy en día. Las interrupciones en la operación, que amenazan la continuidad de los negocios, los accidentes provocados por una amenaza cibernética, el acceso a este tipo de operaciones por amenaza humana, las características del mercado laboral, la automatización de las cosas y el descontento generalizado de carácter social, son algunos de los riesgos a los que se expone el mundo ante esta nueva consecuencia de la cuarta revolución industrial.

María Del Pilar Sáenz R.
Coordinadora de Proyectos
Fundación Karisma
Lo primero es hablar del rol de la sociedad civil, la cual está llamada a prender algunas alertas ligadas al tema de seguridad; particularmente, a los temas asociados con la privacidad, pero no son las únicas. Una de las cosas que hemos estado viendo de forma preocupante es que, en la primera política pública que hubo en Colombia sobre temas sobre ciberseguridad -el Conpes de 2011-, se perdió por completo la oportunidad de que la sociedad civil participara en forma activa en su elaboración; en 2016, para el nuevo Conpes de seguridad digital, sí nos invitaron. Lastimosamente, aun cuando en el nuevo Conpes se advierte que la sociedad civil es importante, que la seguridad digital tiene que ver muchísimo con el análisis de riesgos, que todos somos parte de las soluciones y

de los problemas que hay responsabilidad compartida, en el programa y el desglose del programa, se nombra el marco de derechos humanos, pero no se desarrolla. Entonces desde el punto de vista de sociedad civil, hace falta un montón de controles, primero para algunas de las instituciones que tienen en sus funciones seguridad, privacidad, defensa, inteligencia y demás. También adolecemos de datos; a diferencia de muchas de las partes que están en este debate, que saben cuántos son los afectados en empresas o en bancos por el último ataque, yo no puedo saber. Si vamos a ver cuántas personas fueron afectadas, ni idea; cuántos medios de comunicación, periodistas, cuántas universidades, otro tipo de información, no existe. Y pareciera que no hay nadie que esté encargado de recogerla. Entonces para mí eso es un riesgo y una amenaza y claramente la idea es poderlo debatir también.

Mauricio Guerrero C.
Profesor asociado, investigador
Universidad EAN

Hay tres puntos que me parecen importantes en términos de riesgos. El primero es cómo la diplomacia empieza a convertirse en un tema de diplomacia digital y cómo gracias a que muchas veces se borra la diferencia entre lo que hacen los países y lo que hacen *hackers* rusos o *hackers* de otros países. Esta diplomacia va a comenzar a tener unas implicaciones y unos riesgos en términos de seguridad del sistema internacional. El segundo punto, es cómo esto también va a llevar a que algunos países, si no siguen el ritmo o no implementan sistemas de ciberseguridad en sus fronteras, van a ser Estados en los cuales no solamente va a haber fallas físicas, sino fallas de seguridad. Y se van a convertir en sitios seguros para mafias internacionales o para potenciales personas que vayan a atentar contra la seguridad física, desde la seguridad virtual. Un tercer punto, que me parece un riesgo esencial, no solo en Colombia, sino a nivel mundial, es qué vamos a hacer con la educación. Cómo vamos a formar a esos 18 o 20 millones de personas que vamos a tener de brecha entre lo que requiere el mercado y lo que se está generando, no sólo en las carreras de ingeniería y otras disciplinas, sino en términos legales y económicos; cómo vamos a responder a esa masa crítica que necesitan las sociedades para poder enfrentar este reto de la ciberseguridad a mediano y largo plazo.

Andrés Aguilera C.
Profesor asociado, investigador
Universidad EAN

Frente a los nuevos riesgos de amenazas, me gustaría hablar de Internet de las cosas. El hecho de tener más dispositivos conectados, implica nuevos vectores de riesgo. Me parece oportuno recordar lo sucedido en octubre de 2016, cuando ocurrió un *Distributed Denial of Service Attack* (DDoS), a la empresa norteamericana Dyn. Este ataque fue bastante interesante, porque el método que utilizaron fue a través de la manipulación de cámaras conectadas a internet que habían sido fabricadas en Taiwan; este evento puede ser catalogado como uno de los mayores *DDoS* en los últimos 12 meses. A medida que agregamos más dispositivos, estos se convierten en nuevas avenidas o formas de atacar a los ciudadanos, a las corporaciones y al sector público, entre otros. Evidentemente, esa proliferación de dispositivos electrónicos es

una gran oportunidad de negocios, pero al mismo tiempo tales dispositivos conectados, nos pueden poner en riesgo a todos, tal y como se evidenció en el ejemplo del ataque mencionado.

Hay otro riesgo que hemos detectado desde la academia y lo hemos identificado como el *insider threat*. En algunas ocasiones hemos visto cómo los empleados de una corporación voluntariamente deciden vulnerar sus sistemas de seguridad y es muy poco lo que las compañías hacen para mitigar este riesgo, al menos en Colombia. Cuando hablamos de corporaciones grandes, esas buenas prácticas internacionales se empiezan a establecer acá. Pero, la mayoría de empresas medianas y pequeñas no tienen esa cultura de ciberseguridad.

Y otro aspecto es el cambio generacional que está ocurriendo con la fuerza laboral. En los próximos años la mayoría de la fuerza laboral va a ser ocupada por *millennials*, una generación que nació y creció con dispositivos electrónicos disponibles, pero lamentablemente, no tienen la suficiente conciencia para manejar la seguridad informática. Ellos que, son la mayoría de nuestros estudiantes de la universidad EAN, tienen dispositivos para todo, teléfonos inteligentes, televisores súper avanzados, están en todas las redes sociales posibles, pero son una generación descuidada en términos de seguridad. Son muy pocos quienes son conscientes de los riesgos a los que están expuestos a través de toda esta multiplicidad de aparatos y plataformas.

Juan Mario Posada D.
Gerente de Asesoría
EY (antes Ernst & Young)

Debido al escalamiento de la guerra cibernética que estamos viviendo se requiere un cambio cultural profundo. Los profesionales en temas de ciberseguridad, desde hace muchos años venimos advirtiendo la posibilidad que hoy se ha hecho una realidad. Hace mucho dejamos de enfrentar a jóvenes *hackers* más motivados por un reto, por un desafío académico y de habilidades, que por el dinero o el deseo de hacer daño. Ahora es evidente que nos enfrentamos a organizaciones dedicadas de lleno al cibercrimen, más sofisticadas, peligrosas y con autonomía financiera.

Teniendo claro este contexto, resulta importante mencionar que esta transformación digital empieza a tocar el corazón de los negocios. Estábamos acostumbrados a hablar, por ejemplo, de tecnologías de información asociadas a procesos de soporte; los sistemas que utilizamos cotidianamente como el correo electrónico, el sistema de información financiera, el sistema que gestiona la nómina, entre otros; hoy vemos cómo los riesgos de seguridad se materializan en el mundo de las tecnologías de operaciones (PLCs, SCADA, DCS, etc.).

Esta situación nos ha llevado a una convergencia entre dos mundos soportados por herramientas tecnológicas, pero con prioridades muy diferentes. El mundo de tecnologías de operaciones toca el corazón de los negocios, de las empresas y sus líneas de producción (gas, energía, petróleo, productos de consumo) y, en algunos casos, incluso la seguridad digital de las naciones, como sucedió en Ucrania en el 2016, interrupciones del suministro energético a causa de un ciberataque. Los ciberataques ya no se

quedan simplemente en el secuestro de información, sino que pueden causar desastres ambientales, pérdidas humanas, destrucción de equipos e instalaciones de alto costo en cualquier sector de la economía, lo cual conlleva altos costos de reparación, pues evidentemente reparar un computador portátil no se compara con reparar una planta energética y, tal vez lo más importante, el daño que se le causa a la reputación de las empresas afectadas, pues recuperar la confianza de la sociedad es tal vez lo más difícil de lograr después de un ciberataque.

Jaime Eduardo Santos M.
Vicepresidente legal de Gobierno Mercantil Colpatria
Colpatria S.A.
Desde del mundo del gobierno corporativo tengo una visión holística adicional. Si estamos viviendo la tercera guerra mundial, la ciberguerra es parte de ella. Si uno hace una suma de variables en este momento, encontramos situaciones como la de Siria, en la cual hay al menos 14 países que viajan a bombardear. En las guerras anteriores, se decía que si cinco países entraban en conflicto en dos continentes, teníamos una guerra mundial. Ahora eso está excedido en extremo, esa es una primera variable que me llama la atención. En Siria se usan drones *big data* y también armas biológicas, y eso tiene que ver con la cuarta revolución industrial: nanotecnologia biotecnología, información y cognición.

La segunda variable son las migraciones o desplazamientos como los llamamos en Colombia, las cuales son mayores que en toda la historia de la humanidad. Tenemos migraciones del África empujando duro a Europa Mediterránea y de Europa Mediterránea hacia arriba; encontramos un mesero español en Finlandia. Otra variable que me llama la atención es el crecimiento económico mundial, propio de la recesión de guerra. Esos crecimientos que tuvimos de 4, 5 en Perú o los de China de 8, no se van a volver a

ver en años, según dicen los economistas. Y eso implica otra variable propia de las guerras, el estancamiento o la recesión. Así mismo, los líderes globales que tenemos. En Colombia, con un problema tan serio de liderazgo, lo que estoy sintiendo es que estamos en las mismas que los líderes en resto del mundo. Entonces en conversaciones con mi hijo, le digo, no es que en Colombia hayamos mejorado, es que los demás han empeorado significativamente. Y todo eso me lleva a pensar que estamos viviendo una revolución social. Además, la brecha entre ricos y pobres también es enorme y viene indignando a muchos.

De manera que si uno hace esa combinación de variables o esa mirada sistémica obtiene un marco de actuación muy propicio para que en la cuarta revolución ocurran cosas que jamás nos hemos imaginado. Desde el mundo del gobierno de los ciudadanos creo que la democracia se acabó. Y en cualquiera de las elecciones que veamos, la democracia no existe, porque vota el 30% de la población o la población es obligada a votar, o vota el 70%, pero bajo engaños estadísticos. Y uno de los aspectos que más me preocupa hoy en día es la falsedad en la información estadística, unida a que nosotros tampoco sabemos leer estadística y nos dejamos engañar como mucha facilidad. Uno lee muchos artículos y textos sobre esto y hablan de tener democracia con la cuarta revolución industrial y yo creo que la democracia es la peor opción que se puede tener, cuando pasamos a un mundo en el cual se está cambiando a la propiedad común, al trabajo colaborativo. Así, la democracia está planteada con instituciones competitivas como el mercado y con derechos individuales como la propiedad intelectual y el *habeas data*, yo creo que eso ya debe evolucionar a intereses comunes.

Lo que está operando eficientemente en nuestra sociedad de la cuarta revolución es la anarquía para todo lo analógico y digital. Recordemos, para dar un ejemplo, la calle 72 con carrera 13 en Bogotá, durante una manifestación universitaria; todo es caos, pero todo el mundo pasa la calle. Esto lo explican las leyes de la física, a través de la entropía y en el espacio digital acontece lo mismo, la anarquía tecnológica, porque están ocurriendo cambios tan rápidos, que nos están llevando a ver el mundo de otra manera, como decimos los abogados, en otras circunstancias de modo, tiempo y lugar. ¿Será que el tiempo si existe? ¿O será que estamos todos en el mismo momento? Todo eso lo hace a uno pensar en aspectos que cambia la tecnología. En mi opinión, el siguiente modelo de gobierno que debíamos pensar es el modelo de la "sinarquía", o sea sin anarquía. En mi experiencia cuando se da una crisis tecnológica, lo único que se tiene garantizado es el caos. Y el éxito de la organización es salir lo más rápido posible y con los menores daños posibles de este. Si uno se pone a observar lo que sucede en Internet, ve que de ahí está saliendo la nueva forma de gobierno que es de cooperación descentralizada, en la que es más importante el acceso y el código abierto, que la propiedad privada del mundo analógico precedente y fuerte en las instituciones jurídicas globales. Incluso se puede ver que marcas como IBM, con su inteligencia cognitiva en Watson, permite que los científicos y médicos compartan su conocimiento en oncología. Para resumir, hay que mirar con atención la for-

ma de gobierno que vamos a tener por el impacto de la cuarta revolución industrial.

Jeimy J. Cano M.
Esta primera pregunta de los riesgos deja marcado un poco el terreno en el que nos vamos a mover. ¿Esos estándares y prácticas de seguridad y control van a cambiar? Nosotros veníamos de una tradición en seguridad de mucho tiempo. Si ustedes quieren mirar hay un documento recién desclasificado del Departamento de Defensa norteamericano, fechado el 11 de febrero de 1970[2], donde estaba el detalle completo de cómo se hacía seguridad y control en los sistemas de información del Estado norteamericano. Y si lo revisan a la luz de las prácticas de hoy, la pregunta que este servidor se hizo fue: -¿Será que no hemos evolucionado? Luego de revisarlo la reflexión fue: ¿Casi todo es lo mismo?

En este nuevo contexto la pregunta es ¿los estándares y las prácticas van a cambiar?

Mauricio Guerrero C.
Lo primero que tenemos que cambiar para aplicar estándares y prácticas nuevas es tener mentalidad siglo XXI. ¿En qué contexto? Soy un convencido de que nosotros todavía tenemos sistemas que están actuando para una sociedad estática, cuando estamos viviendo tendencias de dinamismo. Y para poder tener estándares de dinamismo, debemos pensar en lo que no están pensando nuestras Pymes; por ejemplo, cómo abordar mejores prácticas en tests de penetración, cómo incentivar la seguridad de sus bases de datos, no en el mismo lugar, sino mediante redundancias. Adicionalmente, las empresas deben ser capaces de identificar que se están presentando ataques desde adentro, porque siempre se está pensando en los ataques externos, pero no se protegen de los empleados insatisfechos. Para poder cambiar estas prácticas y estándares de seguridad, primero tenemos que cambiar culturalmente. No tenemos que pensar en silos de ingeniería de sistemas, de economía, de sociología, tenemos que comenzar a ser más holísticos en nuestro conocimiento y comprender que hasta que nosotros no identifiquemos cómo estamos educando y cuáles son esos puntos clave de control para empleados y sistemas, no vamos a tener estándares adecuados para nuestras sociedades.

Juan Mario Posada D.
Estudios de seguridad en Colombia muestran que los ciberataques han aumentado en una cifra cercana al 30%. Sin embargo, el más reciente informe global de ciberseguridad de EY, para el caso de Colombia en particular, indica que cerca del 50% de los encuestados declaran que se está disminuyendo el presupuesto en el fortalecimiento de la ciberseguridad y el deseo de protegerla. Lo que claramente va en contravía del cambio profundo de las prácticas, en materia de seguridad de la información. Definitivamente la interconexión es cada vez mayor, por ejemplo, se dice que el ser humano lee hoy cien veces más de lo que leía hace 20 años.¿Qué leemos? Y es importante responder esta pregunta, porque si tomamos las decisiones basados en lo que leemos y lo que leemos no tiene la calidad sufi-

2 Documento disponible en: https://www.rand.org/pubs/reports/R609-1/index2.html

ciente para soportar una buena decisión, estamos enfrentando un caos del que debemos tratar de salir y ese es el desafío interesante. La inseguridad está permeando la relación empresa-cliente, que se facilita por la necesidad de una mayor interacción entre los distintos segmentos de redes. En la industria vemos que hay más convergencia entre las tecnologías de operación y las tecnologías de información para obtener una mayor y más oportuna recopilación de datos que requieren análisis y que soportan la toma de decisiones. También es importante considerar la calidad de dicha información. Con esto quiero transmitir la necesidad de un cambio en los estándares de control. Ya no estamos enfrentados a los mismos riesgos, ni en las mismas condiciones y sí estamos ante un mundo mucho más indiferente y apático a las consecuencias de una guerra cibernética en curso.

Marcela García C.
Somos una empresa que existe gracias a la tecnología y genera flujo de caja gracias a la data que manejamos, pues, sin que entreguemos los datos, sí podemos analizar cómo están consumiendo los usuarios y, eventualmente, ayudar a los proveedores y aliados a entender a sus consumidores. Sin embargo, nunca debemos dejar de insistirle a nuestros empleados en la importancia de resguardar la infomarción y proteger la data. Es imprescindible que todas las empresas hagan lo mismo y que no se entienda esto como algo de las directivas. Mi edad me hace más positiva en el sentido de que tiene que haber un cambio de paradigma. Tiene que haber un cambio de mentalidad para que todas las empresas entiendan la importancia de la información. Sería interesante poner a funcionar métodos de educación para la gente que trabaja dentro de las empresas, y que esto venga como una directriz desde la dirección de la compañía, para lograr que los empleados entiendan la importancia de la información. Un empleado inconforme tiene un arma caliente en su mano que puede dañar la imagen de una organización.

Andrés Aguilera C.
Estandarizar implica cooperación. Y lo que nos ha demostrado la realidad, es que hay desconfianza. Desde la salida de Edward Snowden de su posición como contratista de los servicios de inteligencia norteamericanos, se empieza a filtrar información sobre el alcance de los programas y a generar una desconfianza entre varios gobiernos, por ejemplo Alemania o Brasil. Eso es un punto de partida, pero traigamos la discusión al día de hoy; se está diciendo que *WannaCry* es un subproducto o un rédito de una vulnerabilidad que había desarrollado el NSA, llamada Eternal Blue. Entonces, construir un estándar cuando hay este nivel de desconfianza es complicado. Yo soy un poco pesimista con esta situación. Uno ve cómo se empiezan a generar islas, feudos; vemos países menores como Corea del Norte tienen suficiente poder para desarrollar armas nucleares, o para poner a una empresa como Sony Pictures, bajo un ataque cibernético bastante fuerte, por una tontería. (La película "*The Interview"* no es mala, es pésima). Pero bueno, para discutir esto, está el dilema de estandarizar, porque para estandarizar en un mundo donde hay una desconfianza total, es muy complicado. Así mismo, la mayoría del tráfico de Internet pasa por Estados Unidos y este país tiene una de las legislaciones

más invasivas a la privacidad, esto en sí mismo se convierte en una disuasión a cooperar. Otro aspecto en cuanto a la cooperación, es el alcance que tienen los ataques cibernéticos de hoy. Y la forma de mitigar o de contrarrestar los ataques cibernéticos es a través de la legislación nacional. Pero, infortunadamente, la Ley 1273 del 2009 en Colombia se queda corta, es obsoleta y existen legislaciones en otras latitudes que la superan. Los cibercrímenes no están localizados en una sola jurisdicción, pueden estar enmascarados en un país de Medio Oriente o en una isla del Caribe. Bajo esa perspectiva no hay una estandarización del marco legal, aunque se hayan intentado cambios al respecto. Adicionalmente, hay una brecha muy grande entre los técnicos y la gerencia de la mayoría de las compañías, la dirección todavía no comprende la importancia ni el riesgo al que se están enfrentando.

Jeimy J. Cano M.

¿Necesitamos una alfabetización digital?

Algunas veces los ingenieros no logran que el mensaje llegue a la gerencia. La gerencia está pensando en términos del retorno de la inversión, de cuál es la ganancia o la pérdida del trimestre y estos elementos que son un poco más estratégicos, que son de más largo plazo, no permean el pensamiento estratégico de las compañías. La gerencia todavía ve con desconfianza la inversión en seguridad, porque lo define como un gasto adicional; la ciberseguridad implica costos que la gerencia no quiere asumir.

María Del Pilar Sáenz R.

Efectivamente, sí estamos ante un momento en el que ha cambiado la forma de tomar decisiones, y donde también los gobiernos se están quedando cortos, porque además tenemos un problema al considerar las fronteras. Pensando en un ciberataque, una compañía que tiene negocios en múltiples países.

Un concepto que viene desde la misma Internet, muy útil para esta discusión es el concepto de gobernanza y también el modelo de múltiples partes interesadas. Esas dos cosas que pueden tener todos los peros de este mundo, pero que es bueno traerlas a esta discusión. Porque si bien, estamos acostumbrados a un gobierno centralista, paternalista, que es el que toma las decisiones por sus ciudadanos, por sus empresas, por su institucionalidad. Ahora estamos cambiando a un modelo donde esta misma anarquía y el hecho de que haya más conocimiento repartido, hace también que haya ciudadanos y empresas que quieran participar en esa toma de decisiones y, claramente, todos tienen o todos deberían tener cabida en la mesa donde se discute, sin quitarle el papel al Estado, encargado de legislar o poner un marco de referencia; pero, los otros actores tienen que estar involucrados. Esa es la idea de modelo de múltiples partes interesadas.

Si tomamos eso y lo llevamos a la parte de estándares y prácticas, yo creo, que los hay muy buenos en el sistema financiero, por nombrar alguno. No serán los mejores, no serán perfectos, pero son mejores que los de otros sistemas y, sin embargo, son tan desconocidos para el resto, que es difícil llegar a ese mismo nivel por parte de la sociedad civil, la academia o cualquiera de los otros grupos, que deberían estar implementando sus medidas de seguridad para protegerse. Y es un

problema que no tengamos un estándar abierto, que no tengamos información, que no tengamos estadísticas, o que no las sepamos leer.

La educación juega un papel vital, pero va mucho más allá de la alfabetización. El grave problema que nosotros tenemos, es que hemos dedicado mucho tiempo a enseñarle a la gente a prender el computador, a abrir la hoja de cálculo o el procesador de palabras favorito, y creer que es suficiente y que el usuario ya sabe todo lo que debe saber. En mi concepto, la alfabetización debe apuntar a que los usuarios también conozcan asuntos básicos de seguridad digital, como saber identificar un sitio seguro para navegar en la *web*. Aunque en este tema hay otros problemas, como que el gobierno, por ejemplo, ni siquiera ofrece la mitad de sus servicios a través de páginas con https. Y, más allá de eso, coincido también en que estamos perdiendo interoperabilidad y aumentando la centralización, factores que son bastante nocivos. Las grandes compañías que manejan la comunicación de billones de personas, WhatsApp, por ejemplo, corren el riesgo de que el sistema se caiga y entonces, el mundo se detiene, aparecen los "memes" y la gente se ríe de lo sucedido. Pero, lo grave es la centralización de los canales de comunicación y la falta de interoperabilidad. Para citar un ejemplo concreto, quien usa Signal o Telegram no pueden comunicarse con los usuarios de WhatsApp. ¿Por qué? Porque se creó una barrera y ésta es completamente artificial. Deberíamos empezar a pensar en una estandarización que nos lleve a poder tener interoperabilidad y que el usuario diga, no voy a usar WhatsApp más, quiero usar Signal; pero que esto no impida que fluya la comunicación con los parientes y el experto en seguridad. Así mismo, en términos de las brechas del conocimiento, no es solamente que el técnico no le pueda hablar a la gerencia. Soy una convencida de que éste muchas veces le habla con sinceridad a la gerencia y la gerencia no sólo no lo entiende, sino que no tiene cómo entenderlo. Hay un problema de traducción del lenguaje técnico al lenguaje coloquial. Y si no miramos seriamente cómo logramos hacer puentes, seguiremos creando islas. En resumen se necesitan estándares y buenas prácticas, saber qué está haciendo el otro, mirarnos con un poco más de confianza y ver cómo podemos colaborar.

Sara Gallardo M.

Llevo 19 años como editora de esta revista y en todo ese tiempo no he dejado de escuchar el mismo planteamiento en torno a las carencias de la comunicación entre los técnicos y quienes no manejan el lenguaje de los bits y de los bytes.

Jaime Eduardo Santos M.

Tengo dos aproximaciones frente a la alfabetización digital. Una es que creo que sí van a cambiar todos los estándares, pero a partir de dos cosas. La fabricación de materiales por los humanos, entiéndase materiales como el grafeno y lo que son los seres humanos (biometría) y no de lo que saben o portan. Es decir, cuando uno va a un cajero, tiene una tarjeta y se sabe una clave, eso ya se murió. Pasamos a biometría, que es tomar una parte del ser y después vamos a pasar a partes más internas de ese ser. En este momento estamos en la parte externa del cuerpo, y la siguiente evolución va a la parte interna. Pero, esos estándares vienen por la industria, desde el mate-

rial y el diseño; nos va a gobernar la seguridad y eso va a ocasionar unos tipos de problemas, como los que está planteando la sociedad civil. En otras palabras, vamos a estar atrapados por alguna de las marcas globales.

Lo otro es el tema de confianza, relacionada con los empleados y tiene que ver con el hecho de compartir. En mi opinión, la tecnología está rompiendo la brecha de desconfianza; basta mirar cómo opera *blockchain*.

¿Por qué uno usa un abogado? Porque el abogado debe saber algo sobre normas y jurisprudencia que yo no sé. Es decir, el abogado es un intermediario. ¿Por qué utilizo un comisionista de bolsa? Porque él debe saber algo de mercado que yo no sé, y ahí estoy dispuesto a pagar un "peaje". En general, todo el que está atravesado en la mitad, lo que genera es confianza. Entonces por eso, las instituciones financieras tienen unas supervisiones especiales, unas normas especiales, porque el Estado tiene que cuidar la confianza en la banca central, la confianza en los bancos.

Mauricio Guerrero C.
Todavía tenemos problemas con el cambio en el modelo de negocios de las organizaciones; todavía pensamos en modelos de negocio del siglo XX, y hasta que no pensemos en cómo vamos a cambiar nuestra oferta y cadena de valor para tener en cuenta todos estos temas, muy probablemente va ser imposible que pensar en cómo vamos a sacarle beneficio a la ciberseguridad, a mediano plazo.

Jeimy J. Cano
¿Qué tipo de cambios normativos se advierten sobre el tratamiento de la información, en el marco de la cuarta revolución industrial?

Marcela García C.
El modelo de negocio nuestro gira alrededor de saber interpretar la información, pues aunque generamos rentabilidad con el porcentaje de utilidad que Rappi le genera a los restaurantes y mercados, nuestra labor es estar presente en los micromomentos de los usuarios y, por ende, poderles ofrecer lo que necesitan. Es por esto que es muy importante tener protegida la información, pues nosotros necesitamos tener protegida nuestra data que entiende a los usuarios. Para convertirnos en una aplicación disruptiva, debemos generar confianza y tener un control muy grande de la información que manejamos. Una empresa como Snapchat, que debía algo así como 500 millones de dólares, cuando entra a la Bolsa, se convierte en una empresa de 25 billones de dólares. Y eso se debe a la información que maneja, a que conecta a las personas y a que genera confianza. El poder hoy no lo da la tierra, como en la época de la agricultura. No es quien más tenga fábricas o propiedades, sino quien revoluciona a partir de la información que posee. Si la quinta guerra mundial va a ser por agua, la cuarta guerra mundial será por información. De ahí la importancia de generar una reglamentación básica que no interfiera en el derecho a la libertad de difundir, pero que maneje un control. Así mismo, educar a las personas desde los mismos colegios, sobre la importancia de compartir información y, sobretodo, cómo protegerla.

Juan Mario Posada D.
Aquí hay un tema interesante y es el desafío al que se enfrenta el modelo

legislativo actual de la mayoría de los países. La referencia que hacen a algunas de las aplicaciones móviles y redes sociales emergentes me lleva a pensar en el caso puntual del transporte, con aplicaciones que ya van a completar tres o cuatro años de funcionamiento en Colombia y la legislación aún no resuelve el conflicto, versus el modelo tradicional de transporte público. Es decir, la legislación va a un paso mucho más lento que la transformación digital. Estos problemas se están convirtiendo en problemas sociales de una magnitud importante.

Andrés Aguilera C.

Una de las cosas que ocurren en el sistema legal colombiano, es que lo que no está en la norma, no es delito. Nuestro sistema jurídico deja por fuera lo que no está tipificado en la norma o en el código penal; es decir, no es delito, y en nuestro país, durante muchísimo tiempo, ciertas conductas o actos delictivos que eran ilegales en otro lado, aquí no eran procesados. Precisamente, porque la legislación no había incluido esos nuevos delitos informáticos y como no estaban tipificados en el código penal, entonces no se perseguían.

De otra parte, nos damos cuenta cómo las innovaciones van a una velocidad que deja atrás todo accionar del Estado. Por ejemplo, cuestionamos la legalidad de Uber, a AirBnB porque pone en riesgo la legalidad de los hoteles, que pagan los impuestos, que hacen el registro nacional de turismo y un montón de cosas, estas nuevas aplicaciones empiezan a romper ese modelo tradicional. Sin embargo, las nuevas realidades nos llevan pensar que las jurisdicciones empiezan a borrarse.

Estados Unidos tiene una legislación bastante fuerte de protección al Estado. Uno de los aspectos más interesantes del escándalo de Snowden, es que todo lo que hizo el Estado norteamericano a través de sus agencias, era legal. Ellos nunca quebrantaron la ley. Por eso Snowden sigue siendo considerado un traidor, en lugar de ser un héroe; sigue siendo el "malo del paseo", porque las agencias gubernamentales actuaron dentro de lo que la ley les permitía. ¿A qué voy con esto? Los ciudadanos también necesitan ser protegidos, que se fortalezca el marco legal para protegerlos de la intervención estatal y de la intervención de esas empresas que empiezan a acumular grandes cantidades de datos que ponen en situación de vulnerabilidad la privacidad de las personas.

En Estados Unidos empezaron a implementar las leyes de divulgación. Cuando hay empresas que empiezan a manejar tantos datos sensibles de los usuarios y de los clientes, si llegan a tener algún tipo de vulnerabilidad, el Estado actúa. O sea, cada uno de los 47 estados que al día de hoy tienen leyes de divulgación, obligan a las empresas que han sido vulneradas a notificar a sus usuarios. Eso me parece que es una innovación legal que deberíamos considerar en nuestro país, porque seguramente muchos eventos informáticos ocurridos en Colombia, jamás se han divulgado, precisamente para mitigar el riesgo reputacional de un ciberataque.

Mauricio Guerrero C.

Lo que para nosotros es legal, seguramente para los rusos o para los chinos no lo es y al revés. Entonces, hasta que no sepamos qué es legal en el sistema internacional, los cambios

normativos van a estar relegados a un segundo plano. En este contexto, estamos bien atrasados en términos de comprender en el cómo vamos a combatir cierto tipo de delitos, porque todavía no sabemos cuáles son.

Un punto que me parece muy importante mencionar, con base en lo que han dicho es el tema de criptomonedas, porque no hemos sido capaces de cambiar la arquitectura financiera internacional durante los últimos 25 años, eso lleva un cambio de bastante tiempo y tenemos una nueva tecnología que ha sido disruptiva y está cambiando todo el sistema internacional. Parte del ciberdelito se está generando porque tenemos una moneda que es invisible, que no permite ver quién está detrás de estos delitos.

María Del Pilar Sáenz R.

Hace un año largo, para abril de 2016, Karisma participó dentro de la escuela de sur de gobernanza de Internet, organizada en las instalaciones de la OEA. Y, aprovechando que estaban varios de nuestros amigos y compañeros de la Sociedad Civil de América Latina, decidimos impulsar una declaración conjunta de la sociedad civil a la Organización de Estados Americanos, y a los gobiernos de los países miembros sobre temas de seguridad digital en América Latina. Y es realmente la declaración lo que quisiera traer a colación porque ya está por escrito. De lo que nosotros esperamos, no necesariamente todo se termina resolviendo en la regulación. En algunos casos son acuerdos o marcos generales sobre los cuales operar. Y, en tal sentido, nosotros sí creemos que fue un muy buen cambio, pasar de hablar de ciberseguridad a hablar de seguridad digital en el Conpes. Y es bueno porque el centro lo ponen en las personas y en las comunidades y no solamente en el Estado y la protección de las entidades del Estado. Eso no quita que sea importante la protección de las entidades del estado, pero el centro del asunto debe estar en la gente y en las comunidades. Es decir, debe estar alineado con el marco general de

los derechos humanos de cada uno de los países y del marco global que los cobija. Y ese marco aplica en los medios digitales, de cara a la privacidad, a la libertad de expresión como lo manifiestan los relatores de varios de los organismos internacionales, quienes manifiestan que si no hay una clara ley nacional, existe un marco de derechos humanos internacional que es garantista. En otras palabras, no es posible pasar por encima del derecho a la intimidad de los usuarios para ofrecer sus datos al mejor postor. Y en esa dirección, debe existir una institucionalidad que responda a esas expectativas. Es difícil, pero existe.

Adicionalmente, es necesario adoptar mecanismos de transparencia y rendición de cuentas. Y esto no rige solamente para las compañías que ya lo están haciendo avisándole a sus usuarios cuándo hicieron una petición de datos, sino también a las autoridades mismas cuando retienen información o la solicitan. Y en esta dirección venimos trabajando durante los últimos tres años, en lograr, por lo menos, que las Telcos en Colombia empiecen a generar informes de transparencia basados en la idea de rendición de cuentas. En esta rendición también hay que mirar qué pasa con los macrosistemas de vigilancia frente a los mecanismos de supervisión y control. En el caso colombiano es bastante grave.En nuestra ley de inteligencia y contrainteligencia, se exigió que las Telcos tienen que guardar la información de las conexiones de sus usuarios durante cinco años. En Europa, la Comisión Europea dice que seis meses, es demasiado. Nosotros tenemos cinco años y el acceso a esa información la tienen las autoridades competentes, que finalmente son muchas. Además tenemos cada vez más sistemas masivos de almacenamiento de la información, que pueden generar problemas.

El siguiente paso debería ser un fortalecimiento del cifrado. Nosotros desde la Sociedad Civil, creemos que el cifrado es algo importante y que cualquier tipo de acuerdo internacional para debilitarlo, como tener puertas traseras para burlar los sistemas de cifrado es algo nocivo porque el cifrado garantiza en algunos casos el anonimato, garantiza la posibilidad de ejercer la libertad de expresión y de tener intimidad. Es la batería de derechos humanos, otra vez.

Hay otra cosa que nosotros dijimos en su momento y era que se necesita tener un fortalecimiento y recoger e implementar experiencias y buenas prácticas de otras regiones en materia de políticas de seguridad digital. Y ahí por ejemplo, entra a jugar el tema de Budapest. Si bien no es la panacea y en su momento también tendremos objeciones sobre la forma en que se implementará, sí nos da un marco normativo general que se puede discutir internacionalmente y en el que todos podamos jugar en unas mismas condiciones.

Finalmente, agregaría que independientemente de la regulación que se vaya a plantear en el marco de la implementación del Conpes de seguridad digital, lo que se necesita garantizar es que todas las partes estén ahí en esa discusión, porque sin eso, no funciona.

Jaime Eduardo Santos M.
Abordaré la respuesta como abogado. El profesor italiano Mario Losano tiene un súper artículo denominado “El de-

recho turbulento", en el que señala que ya es hora de jubilar la teoría estructural de Kelsen. Debo anotar para los no abogados que Kelsen es el padre de la pirámide normativa que usábamos los abogados para interpretar el Derecho positivo. Claro que en Colombia no ha muerto la interpretación jerárquica, y las leyes se siguen haciendo pensando que Kelsen aplica en la era digital y al mercado de dos caras o de plataformas tipo Uber. De ahí que en mi blog señale que los abogados debemos cambiar la brújula y la escalera por el GPS. El deber ser es una estructura militar y cuando uno va a la realidad, así no funciona para muchos ciudadanos como los emprendedores del mundo digital. El Derecho es cómo funciona, cómo se vive, cómo lo aplican los jueces y no cómo se escribió en el siglo pasado o antes. Ilustra este punto la jurisprudencia de la Corte Constitucional sobre *habeas data*, que tiene más poder que la ley. También resoluciones de las comisiones de regulación que tienen más poder que una ley. Insisto que debemos seguir las decisiones de los jueces que pueden otorgar o negar derechos. En suma, el Derecho turbulento del profesor Losano exige aplicar el derecho como funciona y no en la jerarquía y la norma.

Además, Colombia no es líder en tecnología, no hacemos ciencia, esto puede sonar duro, pero no estamos en la frontera de ningún asunto de la cuarta revolución. Entonces no podemos estar en normas de frontera, sino en normas de copia, de seguidores. Es importante "darse cuenta" que la regulación en un mundo global viene de ONGs, como ocurre con las normas internacionales de información financiera, o las de gobierno corporativo y más aún, las de industrias como la aviación y la química.

El mensaje que les quiero dar es que los abogados estamos en un mundo turbulento, que empezamos a darnos cuenta que a nuestras facultades de derecho les está pasando lo mismo que a las facultades de contadores y a las de ingenieros; están formando personas para el siglo XXI con herramientas del siglo XX y estamos haciendo mal la tarea de educación, al punto que puede hoy ser más útil una certificación que un título universitario. Este es un debate para hacer.

Marcela García C.

No podemos tapar el Sol con un dedo. Esto es algo que está pasando; los negocios se hacen con información y por eso es importante dedicarnos a educar. Al educar a la gente, al enseñarles la importancia de proteger la información y de tener claridad de lo que implica hacer parte de la era digital. Por ejemplo, si educamos a las personas para que sepan lo que están firmando cada vez que entran a una nueva red social, tal vez, podamos evitar problemas en el futuro.

María Del Pilar Sáenz R.

Uno de los aspectos que considero vital es pensar, así como se planteaba aquí que la democracia ha muerto, uno también podía decir tranquilamente que el consentimiento informado no es suficiente y que eso es una falacia. En otras palabras, el hecho de firmar y marcar la casilla, no son aspectos suficientes para considerar que se entienden y aceptan los términos y las condiciones de servicio. Eso es 'carreta'. Nadie se lee la letra menuda, nadie. Y si tiene lupa tampoco le alcanza la vida para leerse los contratos de las cosas

que firmó cada vez que abrió una cuenta. Además, no lo va a entender porque está en unos términos espantosos. El consentimiento informado es una falacia. Si ese es el panorama, yo si quisiera traerlo acá, porque es un problema para la seguridad de los usuarios. Se les entrega unos poderes a unas empresas con las que se está firmando un acuerdo y al aceptar uno ya ha entregado el alma, esta vida y la otra. Entonces, eso claramente tiene que cambiar.

Hay un modelo canadiense, que es hablar de privacidad por diseño. ¿Qué pasa si ponemos al usuario en el centro? Pues si el usuario no va a ser el que lee el contrato hasta la última minucia ni va a cambiar todas sus opciones de seguridad a las más privadas, arranquemos al revés, que el estándar sea la privacidad. O sea que de entrada, una empresa no le pueda enviar todos los correos de este mundo, y que si usted quiere un correo, tenga que marcar la casilla.

Tuvimos una discusión álgida con el gobierno cuando estaban empezando a plantear todo el proyecto de carpeta ciudadana, -un proyecto de MinTIC que después cambió de nombre a servicios digitales básicos y ahora a servicios digitales ciudadanos-. La implementación de este proyecto implicará que ciertas empresas puedan tener en sus manos la información que resulta de la interacción entre el Estado y los ciudadanos, en la carpeta de cada ciudadano estará almacenada toda esta información. Per se. Yo quiero que esa carpeta y todo el sistema que la soporta tengan las mejores medidas de seguridad y que tengan las mejores opciones de privacidad por diseño. Ese fue el planteamiento que hicimos a ese proyecto. Desde Sociedad Civil no podemos renunciar a eso.

Jeimy J. Cano M.
Se han referido a la confianza como marco general de la discusión y un poco sobre el tema normativo. Éste señala que la confianza, cuando existe, acelera las cosas, y cuando no, genera limitaciones. Más adelante conversaremos que en seguridad lo que hacemos es un ejercicio de confianza imperfecta, todo el tiempo. Todos nos equivocamos. Así que la idea es ponerse de acuerdo en el umbral de riesgo acordado.

Vamos ahora a pasar al tema que es realmente del Estado. Las infraestructuras críticas o los elementos de la gobernabilidad de una nación. Un escenario que, por ejemplo Rappi, lo debe tener en el mapa de riesgos. ¿Qué sucederá cuando eso pase? Y en otros espacios como los aeropuertos, operadores, los servicios de energía, petróleo, gas y otros similares. Se empieza a pensar en la dimensión de lo que implica estar conectados y funcionando, dependiendo de una infraestructura crítica. Así que la siguiente pregunta es:

¿Qué pueden hacer las empresas con infraestructura crítica de un país, frente a esta realidad? ¿Se debilita el cargo de analista de seguridad en el contexto de la cuarta revolución industrial?

Juan Mario Posada D.
Este tema de las infraestructuras críticas es muy vigente, porque el país está trabajando desde hace bastante tiempo en la identificación de la infraestructura crítica cibernética. Y lo que

requieren, pueden y deben hacer las empresas que operan o que son dueñas de los componentes críticos es, en primera instancia, conocer cuáles son esos elementos de la operación del negocio que forman parte de la infraestructura crítica de la nación. Y, a partir de allí, hacer análisis de los riesgos a los que están enfrentados esos activos de infraestructura crítica cibernética, que dejan de ser un riesgo circunscrito y trascienden a lo que es el riesgo o el efecto adverso que puede causar en la nación, en la sociedad civil, en el medio ambiente, en las personas y en los distintos componentes. Habiendo pasado por ese análisis de riesgos, también será importante esa autoevaluación del control, o de los controles orientados a la mitigación de tales riesgos. Un aspecto fundamental cuando hablamos de infraestructura crítica cibernética, es la cooperación. Porque una empresa como *Rappi* depende de los proveedores del servicio de Internet y éste depende del servicio de energía; y el proveedor de energía, a su vez, depende de la empresa de petróleo y gas, por los combustibles que utilizan para mantener sus plantas-; y, así sucesivamente. Se trata de una cadena interminable en la que todos los actores se convierten en un punto único de falla. Y frente a esta situación se requiere una cooperación muy fuerte, para que los esfuerzos sean coordinados en pro de mantener la continuidad. En Colombia no es una obligación reportar los incidentes cibernéticos a los que se ve expuesta una empresa. De manera que la cooperación es el elemento central de la protección de la infraestructura crítica cibernética.

Sobre la pregunta ¿se debilita el cargo de analista de seguridad? Yo no creo que se debilite, se enfrenta a un gran reto. De ahí que sea necesario entender mucho más del entorno en el que opera y construir empatía con los interlocutores del negocio. Porque el analista de seguridad debe verse desafiado a comunicarse en un lenguaje mucho más claro con la alta dirección de la organización, con el Gobierno, con la sociedad, de manera de lograr la alfabetización digital y la alfabetización en seguridad. Porque la sociedad entiende muy bien los riesgos de seguridad física. Por ejemplo, salgo de mi casa, debo dejar cerradas la puerta y las ventanas; salgo de mi casa y debo apagar la estufa de gas; salgo de mi casa y debo tomar una serie de precauciones. Apliquemos estos conceptos a nuestro comportamiento y a nuestra disciplina en el entorno digital.

Jaime Eduardo Santos M.

La infraestructura no es exclusiva del Estado, no es pública, nuestros gobiernos en Latinoamérica han tenido una ola de privatización de los servicios estratégicos, lo hemos visto en nuestro país en los servicios públicos domiciliarios; las telecomunicaciones, la energía, el agua, la recolección de basuras,etc. También es importante se-ñalar que la infraestructura crítica no es una responsabilidad solamente del sector público, sino de las empresas que están operando como concesionarias.

Sobre el analista de seguridad hay un déficit de talento cibernético a nivel global. No hay los suficientes analistas. No obstante, en el evento de CEBIT, de abril de este año en Alemania, vi utilizar sistemas de inteligencia artificial y realidad aumentada, precisamente para gestionar y mitigar los riesgos inherentes a la estructura críti-

ca. En consecuencia, vemos cómo la misma tecnología está proporcionando nuevas herramientas para mitigar esas nuevas amenazas.

Mauricio Guerrero C.
¿Qué pueden hacer las empresas? Pensar en resiliencia y no en continuidad de negocios ni en gestión de riesgos, sino en algo más integrado. Sistemas resilientes, es un tema que todavía no estamos desarrollando en el país y que deberíamos trabajar muy seriamente, de cara a la infraestructura crítica. Si las empresas son resilientes, el país es resiliente, en eso todavía no estamos trabajando muy seriamente, creo que ahí hay una oportunidad para los consultores y para muchas personas. Considero que esto fortalece al analista de seguridad, en el sentido en que el modelo de negocios, le está exigiendo a las empresas tener a alguien interno, y eso hará que esa brecha de talento siga creciendo, debido a que muchas más empresas van a necesitar a estos analistas; a través de tercerización o teniendo a alguien *in house*, pero el analista de seguridad, por todo lo que hemos hablado, es indispensable en el actual modelo de negocios, y una pieza indispensable para poder enfrentar los retos del futuro.

María Del Pilar Sáenz R.
Siguiendo la conversación, la micro conversación, que fue mirarnos a los ojos y decir: "la infraestructura no está o está acá, pero no nos pertenece como país". Además de la resiliencia, también es importante pensar en la transparencia, en todos los escenarios. Para poder tomar buenas decisiones se necesita información y en cualquier caso, la información tiene que ser lo más veraz, completa y actualizada, lo más cercana a lo que está pasando, como para que uno pueda decidir algo. Si se tiene acceso a esa información, probablemente se podrían tomar mejores decisiones, en un marco de transparencia. Si supiera cuántas empresas tienen problemas de seguridad, no estoy diciendo que me digan exactamente qué empresa, porque entiendo el problema de reputación, pero si supiera cómo está el sector, quizá pudiera tomar mejores decisiones sobre si necesitamos más y mejores regulaciones.

Y frente a la figura del analista de seguridad, también creo que se debe fortalecer. Este perfil empezará a cambiar y se le van a exigir otras cosas. En mi caso, yo no solamente le exigiría que hable en un lenguaje un poco más humano con el resto de la jerarquía con la que tiene que interactuar, sino que le exigiría, que fueran un poco más sensibles con las necesidades del usuario y que se pusieran en los zapatos del otro. ¿A qué va esto? En muchas de las decisiones de política pública se consideran las necesidades e intereses de las empresas o del mismo gobierno pero no las de los ciudadanos.

Tomemos como ejemplo los teléfonos celulares y la cantidad de datos que estos dispositivos generan y la información sobre sus usuarios que se puede derivar de su análisis. Un teléfono móvil cada tres segundos se comunica con las torres de telefonía más cercanas, para encontrar la que le da mejor señal en el eventual caso de necesitar establecer una llamada. Por esta razón, cada tres segundos la red de telefonía celular sabe con bastante precisión, donde está mi móvil y por tanto dónde estoy yo. Más allá de eso,

al usar el GPS mi dispositivo puede saber dónde está localizado el equipo y si uso aplicación para tomar un taxi o plantear la mejor ruta hacia mi destino, también sabría hacia donde voy. Yo no siempre quiero que mi teléfono sepa para dónde voy. Y aún más, si mi teléfono sabe para dónde voy, yo no sé si quiero que la compañía que me provee el plan de datos lo sepa.

En este entorno surge la discusión sobre los algoritmos. Los algoritmos nos están definiendo ahora a nosotros como personas, frente a unos intermediarios, que son esas grandes compañías que tienen un consumo masivo de información de la gente. Uno termina siendo perfilado y caracterizado por un algoritmo. ¿Quién controla eso? Nadie. ¿De qué forma podemos tratar que las personas que diseñan y generan esos algoritmos también sean conscientes de otros problemas como la transparencia, la intimidad, la libertad de expresión, relacionadas con otra cantidad de asuntos? Es necesaria una mirada de derechos humanos porque hay un montón de vacíos que no se están considerando cuando se plantean este tipo de preguntas.

Jaime Eduardo Santos M.
Hay bienes que son públicos, bienes que son privados y bienes que son comunes, como el aire. Entonces lo primero que tienen que hacer las empresas con infraestructura crítica es ser conscientes de que manejan un bien común, no un bien privado. Cada vez que hay un debate, que si unas antenas se tienen que devolver, que si unos camiones de basura se tienen que devolver, se arma un debate, que si eso es público, que si es mío o si es de quien dio la concesión. Entonces, me encamino porque tenemos que proteger el concepto del bien común, que es además una institución real, en el mundo irreal del derecho. Y el que está llamado a que eso funcione así, es nuevamente el ciudadano a través de la democracia participativa. Si bien, atrás mencioné que la democracia murió, es porque la participación ciudadana la está ayudando a que muera, la está ayudando a enterrar. Hay que pasar a la democracia participativa.

En segundo lugar, además de saber que es un bien común, es necesario aprender de la industria de los juguetes para hacer las cosas bien desde el diseño y probarlas en laboratorios que les permitan responder con eficiencia durante una crisis, quizás originada en un error humano o en un ataque cibernético a la energía o las comunicaciones.

Soy un convencido de que en las cosas básicas están las soluciones a las más complejas.

Jeimy J. Cano M.
¿Cuáles son las habilidades, competencias y conocimientos que requerirán los nuevos profesionales frente a la seguridad y control en la cuarta revolución industrial? ¿Se están preparando las universidades para formar a los estudiantes en dichas competencias/habilidades?

Marcela García C.
De la misma manera que se instauró como requisito hablar inglés, se debería exigir a los empleados saber cómo reconocer la importancia de proteger la información y entender un poco acerca del mundo digital. Debemos aprovechar que en el país está llegando Internet a los municipios más apartados, para poder educar a todas las

personas a que administren mejor la información, a saber a qué están expuestos y a aprender sobre cómo manejar la información en el momento en que se vinculen laboralmente a una empresa.

Juan Mario Posada D.

Las dos habilidades fundamentales de los nuevos profesionales deben ser el buen uso de la tecnología y el buen uso de la información, desde el punto de vista de la ética, de la responsabilidad social y, en general, de la profesión de la cual hacen parte. Así mismo, es necesario que los profesionales se preparen en seguridad, frente a esta cuarta revolución industrial. Y puede parecer muy gracioso, pero los profesionales de seguridad tendrán que aprender de mercadeo, de cadenas de suministro, de estrategias, de servicio al cliente, de líneas de producción, de finanzas en una medida suficiente para entender los retos de los negocios digitales, para lograr ofrecer valor a través de la gestión de la seguridad.

Andrés Aguilera C.

Este es un tema que nos toca a nosotros como profesores de la universidad y es una de las líneas de investigación que estamos adelantando. La cuarta revolución industrial implica la desaparición de muchos empleos; implica que muchas funciones se pueden automatizar y se pueden dejar a algoritmos a programas, a un montón de cosas. Y, en tal sentido, el reto de universidad es que seguimos operando bajo un modelo de negocio obsoleto. La misma tecnología nos está retando, porque el salón de clase es una limitación física, cuando vemos que el nuevo modelo negocios contempla el uso de MOOC (Massive Open Online Course), cursos de miles de estudiantes y la pregunta que nos debemos es ¿qué están haciendo nuestras universidades para entrar en ese juego? Entonces el modelo actual, que es el que seguimos, es el profesor, quien prepara su clase, tiene una infraestructura limitada, el número de sillas, el número de estudiantes. Pero cuando el modelo de negocio cambia y se convierte en un MOOC obviamente las posibilidades son mucho más grandes. Y la cuarta revolución industrial también está poniendo presión sobre los profesionales de otras disciplinas.

Estamos viendo tecnologías como *high-frequency trading*, en la que el analista financiero sólo tiene que determinar ciertos parámetros de rendimiento. Tecnologías como la inteligencia artificial o la impresión de 3D van a cambiar el panorama laboral. Todos los pronósticos que se hacen es que nuestros profesionales están aprendiendo al día de hoy cosas, que van a ser obsoletas muy pronto.

La apuesta que estamos haciendo es que nuestros estudiantes empiecen a aplicar algo que se llama *Life-Long Learning*, para que las herramientas que reciben en la universidad les sirvan, no sólo para obtener un grado y un título, sino para que puedan seguir aprendiendo a lo largo de su vida. Todo está cambiando muy rápido. Nuestros profesionales de la próxima promoción, seguramente en muy poco tiempo, tendrán que volver a las aulas o tendrán que volver a formarse en las últimas tendencias, en el más reciente *software*, o en cualquier asunto que sea necesario. La cuarta revolución industrial está cambiando toda la dinámica del trabajo, se está contemplando el desempleo tecnológico y la universidad, de cierta forma, debe lle-

nar esos vacíos, también innovándose.

Mauricio Guerrero C.

En mi opinión, se trata de habilidades. En el informe del Foro Económico Mundial, del año pasado se decía que ocho de cada 10 habilidades necesarias a 2020 serán habilidades suaves, un aspecto muy importante para cualquier profesional. Así mismo, se referían al problema de comunicación que tenemos. Es necesario revisar cómo nos comunicamos todos para tener modelos de negocio más exitosos. Hacia el futuro serán las certificaciones las que funcionen, en especial porque los análisis que estamos realizando lo hacemos bajo el paradigma de la computación clásica, pero una vez la computación cuántica sea comercializable, nos va a cambiar todo.

María Del Pilar Sáenz R.

La pregunta me puso a reflexionar, porque debe orientarse a si hay que formarse para la vida y no para el trabajo. Parece obvio decirlo, pero hay que decirlo. Y lo planteo desde mi propia experiencia. Soy física de formación y todo lo que he hecho durante los últimos años está relacionado con una rama totalmente diferente. Es decir, mi trabajo en la política pública es más de abogados que de cualquier otra disciplina. Y terminé involucrada porque me interesaba. El pensamiento en la "caja" es lo peor que uno puede poner en práctica. Un aspecto clave es la flexibilidad, la posibilidad de iniciar con un tema y terminar en otro, experimentando la formación por el camino. Más allá de tener una serie de habilidades esenciales es importante entrenarse para hacer algo específico. En ese sentido, el aprendizaje sobre tecnología también debe enfocarse no hacia saber hacer, sino hacia entender cómo funciona. Es paradójico que la mayor parte de los equipos utilizados son cajas negras para casi todos los usuarios. Tan es así, que somos incapaces como país de generar una nueva tecnología, porque no la entendemos y no estamos en esa punta. La solidaridad se suma también; puede parecer un valor extraño cuando uno lo piensa en educación, pero es muy importante ponerse en el 'zapato del otro' y ser capaz de bajarse del nivel de lenguaje especializado cuando se le habla a una persona que no habla sobre lo mismo, en los mismos términos. El principio que me enseñaron en la universidad, es que realmente podría demostrar que entendía un tema, cuando fuera capaz de explicárselo a una persona sin conocimiento sobre el área. En pocas palabras, falta mucha pedagogía sobre tecnología.

Jaime Eduardo Santos M.

La formación universitaria daría para un único debate. No obstante, en mi opinión la academia está atravesando por una crisis enorme y opto por las certificaciones. Y a estas sumaría la curiosidad y una visión transversal. Infortunadamente, nuestro sistema educativo es de silos de conocimientos. Si usted es abogado, no sabe sumar; si es físico no sabe leer. Y todas las universidades están construidas desde esa perspectiva. Así que el primer cambio en las personas sería lograr salirse de esas cajas para tomar diferentes asignaturas en diferentes disciplinas. Las universidades no son flexibles, aunque los jóvenes estén optando por hacer dobles programas. Basta contemplar la dificultad para el cambio de una carrera a otra, aunque sea similar en disciplina.

Y además, cuando pasamos a la inteligencia cognitiva de la cuarta revolución industrial, la situación se vuelve más compleja para los métodos de enseñanza tradicionales. La máquina aprende como el humano para ayudarle, pero podría ser para sustituirlo en muchas funciones, como algunas legales. (Abogado Ross basado en Watson). Luego lo que tenemos que legarle a las nuevas generaciones es que sean curiosos y holísticos para construir su historia de vida. Aquí en el foro estoy oyendo dos ejemplos que me llaman mucho la atención: una física en políticas públicas y un politólogo en sistemas. Eso son historias de vida, eso no son hojas de vida.

Jeimy J. Cano

Después de observar los caminos disciplinares, hoy estamos en otro escenario que es el transdisciplinar: comenzar en Comunicación, conectar con Derecho y terminar en computación. Esto significa construcción y conexión. En esa dirección creo que la cuarta revolución nos invita a mirar una postura de tales dimensiones.

Sara Gallardo M. *Periodista comunicadora, universidad Jorge Tadeo Lozano. Ha sido directora de las revistas "Uno y Cero", "Gestión Gerencial" y "Acuc Noticias". Editora de Aló Computadores del diario El Tiempo. Redactora en las revistas Cambio 16, Cambio y Clase Empresarial. Coautora del libro "Lo que cuesta el abuso del poder". Ha sido corresponsal de la revista Infochannel de México y de los diarios "La Prensa" de Panamá y "La Prensa Gráfica" de El Salvador. Investigadora en publicaciones culturales. Gerente de Comunicaciones y Servicio al Comensal en Inmaculada Guadalupe y amigos en Cía. S.A. (Andrés Carne de Res); corresponsal de la revista IN de Lanchile. En la actualidad, es editora en Alfaomega Colombiana S.A., firma especializada en libros para la academia y editora de esta revista.*