Ciberseguridad industrial, seguridad de la información y negocio: ¿encuentro o divorcio?

DOI: 10.29236/sistemas.n147a5

Dos conceptos bien diferenciados por las condiciones actuales que los rodean y los avances tecnológicos.

Sara Gallardo M.

La movilidad, los dispositivos interconectados, Internet de las cosas y la inteligencia artificial –para citar algunos avances tecnológicos- dieron lugar a la gestación de dos espacios bien delimitados en el ambiente actual: ciberseguridad industrial y ciberseguridad de la información y del negocio.

Y aunque pareciera existir claridad sobre el alcance de cada uno, su complementariedad e interacción, lo cierto es que los profesionales en seguridad de la información y seguridad de la operación, muchas veces circulan por caminos diferentes que los distancian y producen un impacto negativo en las organizaciones.

Para debatir sobre los asuntos más relevantes alrededor de estos temas fueron invitados: Leonardo La-

torre Patiño, profesional de Seguridad de la Información y Telecomunicaciones, para la Vicepresidencia de Transporte, en Ecopetrol; Felipe Silgado Quijano, Chief Information Security Officer para el Grupo Scotiabank en Colombia; Juan Mario Posada Daza, Manager Advisory, de Ernst & Young; Wilmer Prieto Gómez, vicepresidente Capítulo Bogotá, de Isaca; y Diego Andrés Zuluaga Urrea, responsable de Seguridad de la Información en Isagen.

"Los asuntos que vamos a tratar hoy forman parte de un tema polémico y son un gran reto en la actualidad –manifestó Jeimy J. Cano M., director de la revista y moderador del foro–. Hoy se dice que los objetos están aumentando su densidad digital, en la medida del papel que juegan las interfases y los datos, hecho que empieza a tener relevancia desde el punto de vista de los negocios", señaló Cano para abrir el debate.

Jeimy J. Cano M.
Moderador
¿Cuáles son las prioridades en la seguridad en el mundo TO (Tecnología de Operaciones)? y ¿cuáles en el mundo TI (Tecnología de Información)? ¿Son distintas?

Juan Mario Posada Daza
Gerente de Consultoría
EY
Las prioridades son distintas y debemos tenerlas en cuenta. Aunque, de cara a la seguridad la base es la misma, es decir, proteger la confidencialidad, integridad y disponibilidad de la información de estos dos mundos. No obstante, el orden de prioridad cambia, porque tradicionalmente en el mundo de TI, la prioridad más alta es la confidenciali-


Diego Zuluaga


Felipe Silgado


Juan Mario Posada

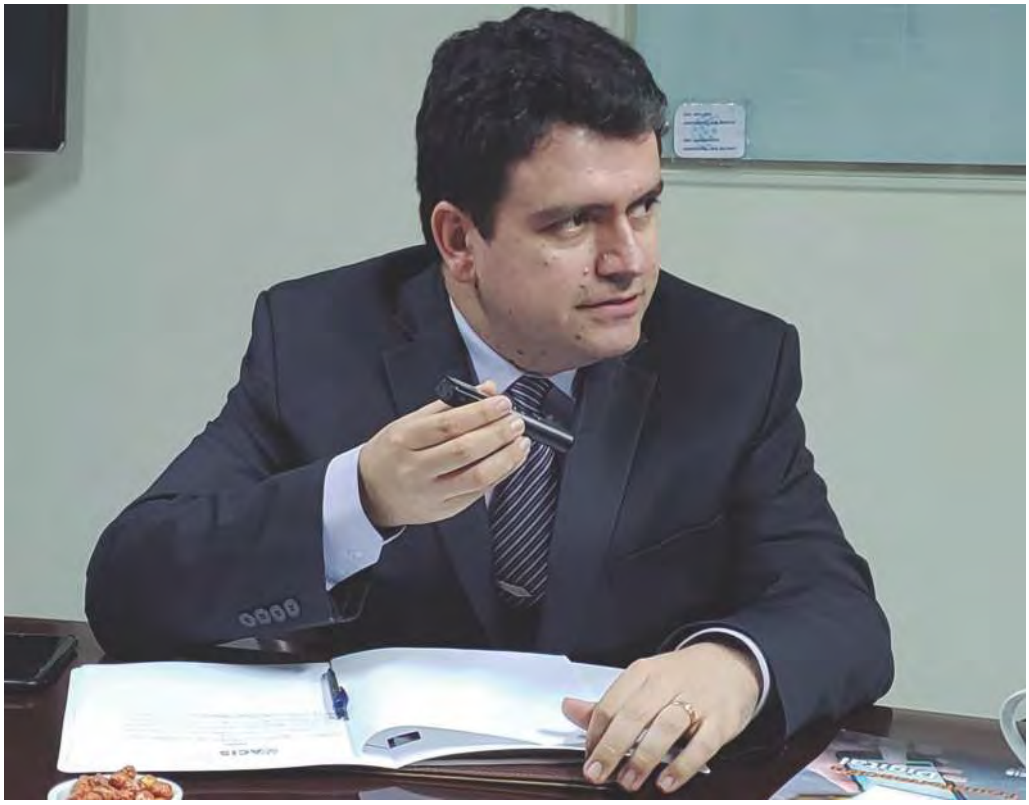

Leonardo Latorre

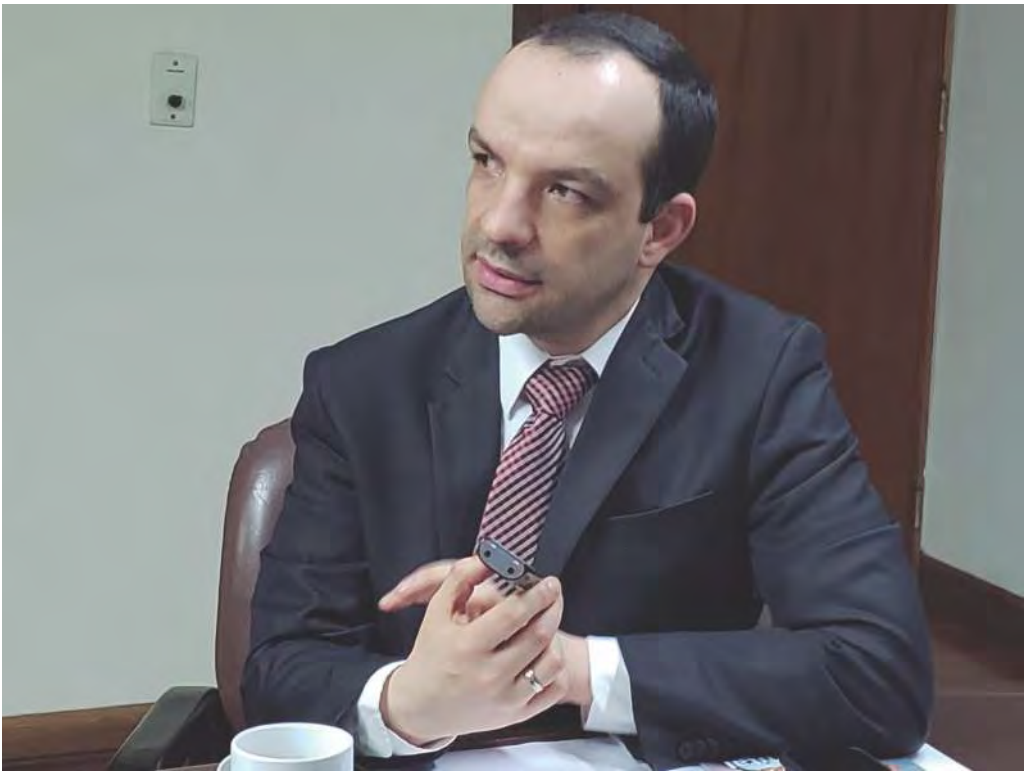

Wilmer Prieto

dad. En el ambiente de las Tecnologías de Operaciones (TO) la experiencia me ha mostrado que se invierte la pirámide y allí lo más importante es la disponibilidad, porque cualquier falla en ese sentido pega directamente a la generación de ingresos de las compañías que se soportan en este tipo de tecnologías, en su *core*. Le apuntan a lo mismo en un orden diferente.

Diego Andrés Zuluaga Urrea
Responsable de Seguridad de la Información
Isagen
Debo informar que todas mis respuestas son opiniones personales.

En este caso, estoy de acuerdo en que la pirámide se voltea y la disponibilidad es mucho más importante en el mundo TO; sin embargo, aparece un elemento adicional para cuidar que es el *safety*, es decir la seguridad de las personas del medio ambiente y de los equipos, porque aquí estamos tocando un tema que las personas del área industrial han desarrollado por muchos años, como es evitar heridas, problemas físicos, que el medio ambiente no sea afectado por un derrame o algún otro evento, entre otros. Además de considerar los impactos sobre los equipos de alta complejidad y difíciles de reempla-





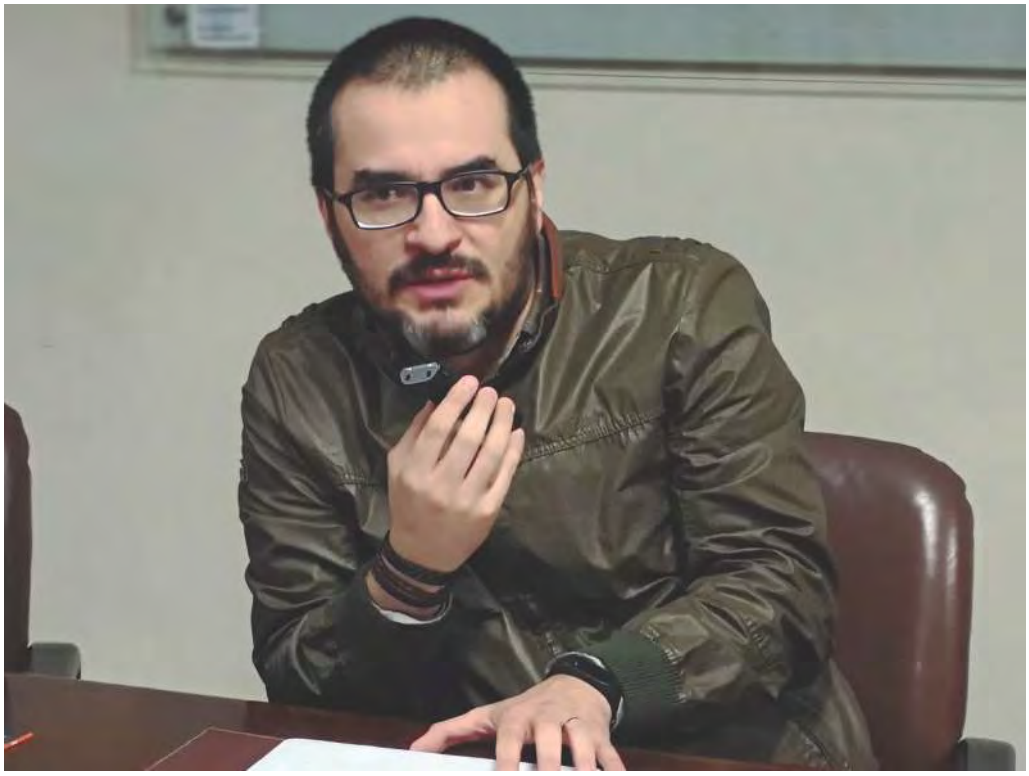
zar, que son de carácter crítico, toda vez que pueden parar el funcionamiento de una empresa o un sector. Y si a esto le agregamos el IOT o Internet de las cosas, en el sentido de plantear que ya contamos con sistemas ciberfísicos en todas partes, incluidas casas y oficinas, y la industria 4.0 ya lo contempla. Así mismo, considerar los datos personales que estos dispositivos obtienen en todo momento y cómo los están manejando las empresas que los mantienen; es necesario contemplar también en este proceso, la nube que maneja los dispositivos físicos inteligentes de la casa, porque la información está en manos de terceros.

Felipe Silgado Quijano
Chief Information Security Officer para el Grupo Scotiabank en Colombia

De cara a la operación, el tema de la disponibilidad. Así mismo, la automatización que lleva a que las tareas se realicen de una manera más eficiente, los controles funcionen de forma más precisa y permanente en el momento en que se requieren, hace que mucho de la operación se oriente hacia ese mundo. Y en el de TI, el manejo de grandes masas de información como Big Data conduce a que los sistemas requieran de un siguiente paso en su evolución, en procura de una disponibilidad y capacidad más al-

tas. Y, por ende, en los sistemas de operación pues requieren sistemas más automáticos, más rápidos y eficientes. En mi opinión, los dos asuntos van alineados, y aunque funcionen de manera independiente van a converger en el mismo punto que no es otro que el manejo de la información para crecer el negocio y cumplir con los objetivos.

Leonardo Latorre Patiño
Profesional Seguridad de la Información y Telecomunicaciones Para la Vicepresidencia de Transporte
Ecopetrol
Las prioridades son diferentes y estoy de acuerdo con lo ya planteado. En tecnologías de operación es indiscutible que la disponibilidad está encima de la pirámide. Como bien mencionaban, cualquier falla en ésta puede afectar el *core* del negocio, para las empresas que utilizan ese tipo de tecnología. Agregaría que las prioridades en el mundo TI y TO pueden cambiar por la reducción tan grande que se registra en la brecha de los dispositivos que estamos usando en tecnologías de operación y en tecnologías de información. Cada vez están más integrados. Antes encontrábamos dispositivos y fabricantes exclusivos de tecnologías de operación y veíamos dispositivos de TI que no había en TO. En la actualidad, encon-



tramos dispositivos que soportan TO, fabricados por empresas líderes en la elaboración de dispositivos de TI. En resumen, la diferencia de prioridades que existe actualmente entre TI y TO puede cambiar, tendiendo a ser igual para disponibilidad, confidencialidad e integridad, debido al cierre de la brecha entre las tecnologías de operación y las tecnologías de información.

Wilmer Prieto Gómez
Vicepresidente Capítulo Bogotá ISACA

Para complementar lo ya expuesto, estamos totalmente alineados en que los criterios de la tríada entre confidencialidad, integridad y disponibilidad son diferentes en TO Y TI. Aparece la palabra ciberseguridad y, en tal sentido, debemos entender que no toda infraestructura crítica TO se relaciona con tecnologías de Supervisión, Control y Adquisición de Datos (SCADA), Servicios de Producción Electrónica (EMS), Sistemas de Control Industrial (ICS), entre otros; hay otras operacionales que son igualmente críticas para otros sectores. En el financiero, por ejemplo, el *core* bancario requiere unos componentes diferentes de seguridad y maneja protocolos tal como lo ha-

cen en TO para entornos operacionales. Protocolos totalmente independientes, con unos niveles de seguridad relevantes. De ahí la importancia que en los diferentes sectores empecemos a adoptar marcos de referencia especializados en el tema de ciberseguridad, en los que se contempla no sólo el aseguramiento del entorno -sea TO o TI-, sino también cuál es la responsabilidad para que desde mis entornos digitales no se pueda comprometer a terceras partes, sea industria, Gobierno o personal civil. Ahí es donde también el concepto *safety* es muy relevante. Así mismo, como se venía exponiendo, la transformación digital es muy importante y es donde a través de las tecnologías TO y TI se genera valor agregado para el negocio. Y como líderes de seguridad debemos pensar en cómo desde las estrategias de seguridad de la organización se genera esa ventaja competitiva de una forma responsable, lo que permite llegar al público objetivo. Otro aspecto significativo es la utilización de marcos de referencia en ciberseguridad que permitan alinear esas estrategias, porque algo que se debe tener en cuenta es que cualquier marco de referencia, sea para infraestructura operacional o para TI u otras, se refiere a transmisión, almacenamiento y procesamiento de datos o de materia prima. Esos tres entornos los tenemos en toda infraestructura operacional o crítica. Se trata entonces de encontrar el balance entre la tríada de seguridad y los demás entornos. Eso mismo funciona en los asuntos de seguridad ciudadana, porque los marcos de referencia de ciberseguridad facilitan hacer inclusivo el objetivo principal que es el factor humano. Las TI y TO son un medio para alcanzar un objetivo, pero éste siempre depende de los seres humanos para lograrlo. De ahí que el tema de ciberseguridad sea tan importante dentro de todo el contexto.

Jeimy J. Cano M.

¿Cuáles tensiones o retos se identifican al hablar de seguridad o ciberseguridad en el mundo TI y TO?

Juan Mario Posada D.

La primera tensión de la que se habló es la diferencia de prioridades de uno y otro mundo. También hay una tensión causada por el entendimiento de las necesidades de cada uno de ellos; tradicionalmente, la administración tecnológica del mundo de IT con el de las TO ha sido por completo independiente y, es muy probable que, hoy por hoy, estos dos mundos se sientan amenazados cuando se habla de convergencia tecnológica, toda vez que dicha convergencia implica la centralización de la administración y la estandarización, entre muchos otros aspectos. Adicionalmente, algunas empresas de cierto nivel de madurez y en algunos sectores de industria esa brecha entre TI y TO

cada vez es más invisible, pero todavía existen muchas industrias que apalancan sus procesos productivos en TO y que ni siquiera ven la necesidad de asegurarlas. Sin ir muy lejos en la industria textil podrían ser contadas con los dedos de una mano, aquellas empresas que han puesto los ojos sobre el aseguramiento de las TO y soportan sus procesos productivos. Obviamente, cuando nos centramos en elementos de la infraestructura crítica de una nación, se produce una especie de lucha de poderes en la que cada mundo (TI y TO) tiene sus necesidades y una visión de la gestión de riesgo, que causa mayor tensión.

Leonardo Latorre P.

Los retos que se identifican en ambos mundos tienen en común varios puntos. Las redes sociales y su manejo en las organizaciones, aunque no estén directamente relacionadas con el objeto del negocio, como es el caso de la industria petrolera, pueden afectar a la compañía en forma notable para bien o para mal. Los dispositivos móviles, porque es una realidad que los directivos de las compañías quieren tener la información de su proceso en tiempo real y en un dispositivo móvil y esto se convierte en una tensión para los profesionales de seguridad de la información. Otro reto grande que está llegando en ambas tecnologías es la virtualización, hecho para el que no estábamos preparados y es una realidad en diferentes empresas. Inclusive, en los sistemas de control industrial. Así mismo, *cloud computing* va de la mano con la virtualización y muchos procesos ya se aseguran en la nube; es un tema todavía en discusión que no está escrito, pero es una realidad que genera tensión y se convierte en reto para TI y TO. La evolución tecnológica hace que la diferencia entre TI y TO sea menor o más gaseosa, en la mayoría de industrias, aunque existen muchas que se mantienen sin ocuparse de tales asuntos. La convergencia tecnológica también es otra tensión que se debe atender con premura.

Felipe Silgado Q.

En el sector financiero se contemplan el servicio y la necesidad de seguridad para prestarlo. En tal sentido, existe un desbalance en relación con lo que busca el negocio, como poner al servicio del cliente las redes sociales para la realización de sus transacciones por Internet desde cualquier punto en donde esté, ojalá sin tener que usar la tarjeta y hacer todo por el teléfono celular. Así que el tema se orienta a la posibilidad de ofrecer un servicio muy amplio hacia los clientes, quienes solicitan que no los restrinjan en el uso de medios y dispositivos para sus transacciones. Eso conduce a unas tensiones. Los reguladores han estado muy estrictos con la producción de nuevas medidas; esperamos, por ejemplo, por parte de la Superintendencia Financiera, una Circular sobre ciberseguridad que va a im-

pactar fuertemente el sector; esta Circular llega después de que la Superintendencia haya realizado una evaluación al sector y detectado la existencia de tantas brechas. Tuve la oportunidad de ver tres tipos de informes relacionados con el sector financiero (banco, fondos de pensiones y fiduciarias) y pude observar las diferencias existentes entre estos tres subsectores. Los bancos están más enfocados en la protección, mientras que los otros tipos de compañías no. Los reguladores están ejerciendo presión para cumplir con las normas. Vienen muchos lineamientos orientados a presentar a la Junta Directiva los asuntos relacionados con la seguridad, para ponerla al tanto de las brechas y los problemas que se avecinan, como Facebook, que afecta a nivel mundial, mega fugas de datos y ataques dirigidos, entre otros. Esa es la tensión que se genera y el reto de cara al balance entre negocio, cumplimiento y control.

Diego Andrés Zuluaga U.

La cultura es uno de los primeros retos a asumir entre los mundos TI y TO. En el mundo TO es común escuchar "lo que está funcionando no lo toque", y en el mundo TI esto no es posible, porque cada día es necesario realizar alguna acción. Por ello, el control de cambios es algo que pueden aprender las personas de TO, es algo positivo, porque garantiza que la disponibilidad va a estar cada vez mejor. Pero, también obliga a que no podamos considerar algunos temas tan fácilmente, como parchar entornos o implementar antivirus con actualización de firmas constantes, así como controles similares que cambian los entornos frecuentemente, cuando éstos deberían ser muy fijos. Las estrategias en este tipo de entornos deben orientarse hacia listas blancas de aplicación, para garantizar que lo que está funcionando continúe así, porque el comportamiento con otro tipo de controles es impredecible y se podría llegar a afectar a las personas, el medio ambiente, los equipos o la disponibilidad del servicio. También debemos considerar el tiempo de vida en las instalaciones de TI, toda vez que hablamos de tecnologías para tres o cinco años y en TO se habla de infraestructura para 15 e inclusive 20 años. Cuando se requiere cambiar un servidor, la pregunta del personal de TO es ¿por qué si lleva poco tiempo funcionando? Se trata de un tema muy complejo. El problema es que ahora, como se mencionaba, se están integrando tecnologías de información a las tecnologías de operación, las cuales están diseñadas para ciclos de vida entre tres y cinco años. Por lo anterior, se genera una tensión entre la necesidad de hacer esos cambios constantes para mantener la seguridad y la necesidad de mantener la disponibilidad y un sistema confiable que tenga una curva de la bañera que dure mucho tiempo en la parte inferior. Enfatizo en la cultura que se debe producir en tales entornos y que podemos aprovechar los avances en

seguridad, porque en los noventas cuando comenzamos a asegurar las TI éramos muy pocos los que nos referíamos a estos asuntos y, hoy en día, para la seguridad industrial tenemos buenos profesionales de la seguridad a quienes es necesario enseñar las diferencias que existen entre TI y TO, porque cuando se llega a las personas de operación con el discurso de TI, se cierra la comunicación. De manera que se debe entender su entorno para utilizar un lenguaje adecuado en el mensaje. Ojalá los profesionales de TI pasaran buen tiempo en planta para comprender ese mundo

Wilmer Prieto G.

Son varias aristas a tener en cuenta. Por una parte, lo relacionado con la cultura y el desconocimiento de los entornos a todo nivel. Cuando hablamos de seguridad no sólo es necesario referirse en términos de organización, sea pública o privada, sino también a cuáles son los sectores de infraestructura critica definidos a nivel nacional y como nuestras empresas hacen parte de los mismos. Así mismo, tener claridad sobre cuáles son las entidades en Colombia que rigen ese sector en particular y cuál es la estrategia del Gobierno en los asuntos relacionados con defensa y dirección. Una de las tensiones más grandes que identifico está relacionada con el desconocimiento. Vemos cómo en los diferentes Ministerios es evidente, toda vez que no pueden complementar desde el punto de vista gubernamental, lo que produce un impacto general. Es necesario trabajar en esa dirección, en cultura digital en todos los niveles. Otro asunto es el cumplimiento normativo y contractual, en donde existe una tensión muy fuerte entre TI y TO, porque los temas contractuales aún tienen muchos grises y no sólo en el país, sino en otras latitudes. Vemos cómo la adopción de la nube y otro tipo de tecnologías nos llevan a observar los requerimientos y contratos que cobijan la confidencialidad, integridad, y disponibilidad de datos e información digital en transmisión, almacenamiento y procesamiento. Se requiere garantizar el buen funcionamiento de tales frentes. Otro tema muy importante es el desconocimiento de la infraestructura operacional. Hace unos 15 años tuve la oportunidad de realizar unos análisis de riesgo e implementación de controles de seguridad, partiendo de TI hacia TO, en una fábrica de producción y desde los requerimientos de seguridad tecnológicos del negocio no se llegaba a comprender lo complejo que resultaría asegurar *hardware* descontinuado tipo servidor, con sistema operativo fuera de soporte, el cual interactuaba con tarjetas controladoras alemanas y Controladores Lógicos Programables (PLC) en las máquinas de producción, para los cuales el fabricante TO no contaba con rutas de actualización a corto plazo (recordemos que los tiempos de renovación de tecnologías TO son mucho más extensos que en TI),

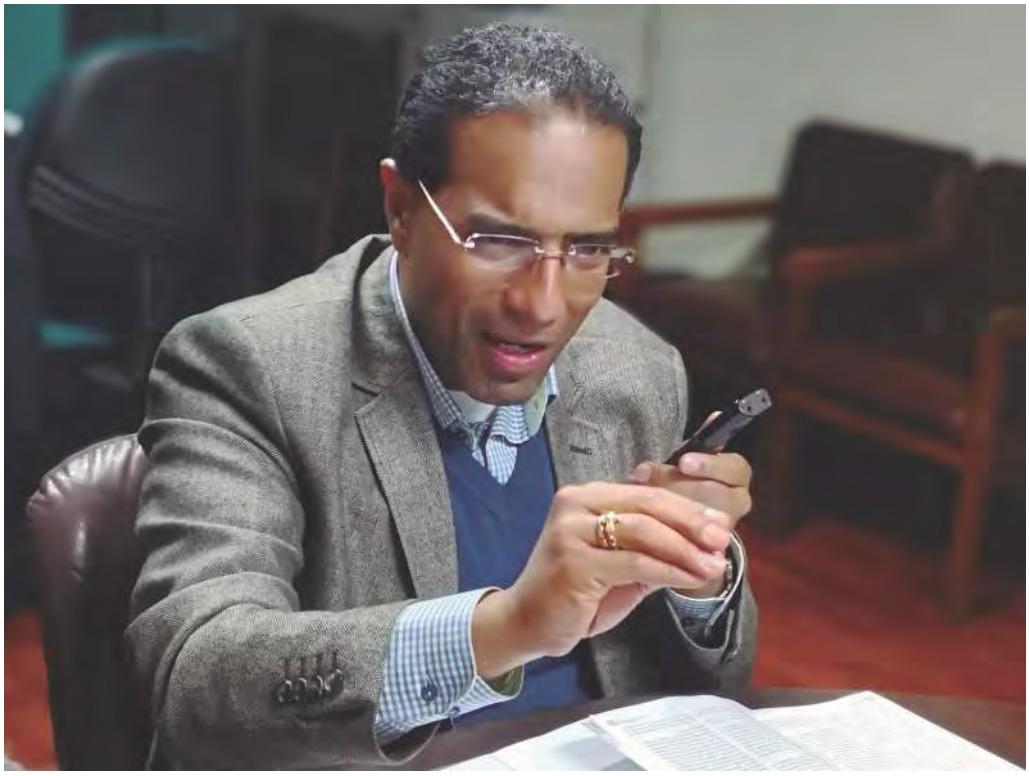
sistemas en los cuales no se podía pensar en controles mitigatorios basados en la instalación de ningún tipo de *software* Anti-x o de endurecimiento de núcleo, ni contar con ventanas de mantenimiento extensas, toda vez que esto se reflejaba en disminución en la producción diaria y en pérdida económica para el negocio. Es necesario entender esos entornos y crear seguridad a la medida, para generar un buen balance entre los diferentes entornos.

Jeimy J. Cano M.

¿Cuáles aspectos se deberían tener en cuenta para construir una vista conjunta de la seguridad y ciberseguridad en TO y TI?

Juan Mario Posada D.

Existen algunos beneficios identificados en la convergencia de los mundos de TI y TO, contemplando algunas de las observaciones aquí señaladas. Por ejemplo, la selección de proveedores para la búsqueda de economías de escala, puede ser interesante para los dos mundos en los que hay presupuestos diferentes, probablemente más amplios en TO, toda vez que los costos de las tecnologías especializadas así lo requieren y soportan el *core* del negocio. Aunque aquí se ha dicho que cada vez son más las adquisiciones tecnológicas comunes o los dispositivos de TI que empiezan a permear el mundo de TO, insisto en que no es una situación



generalizada porque aún existen muchas compañías e industrias cuyos negocios se soportan en TO y que no tienen la conciencia de seguridad y, probablemente, porque la misma regulación nunca ha sido tan estricta, por ejemplo, en términos de *Safety* con ellas, como sí lo son en las industrias de energía, petrolera y otras similares. Uno de los beneficios interesantes que puede haber allí, entendiendo los dos lenguajes, es la estandarización de procedimientos de seguridad, según aplique. La integración y optimización de procesos que promuevan la eficiencia, es otro aspecto a contemplar. El aprovechamiento de las competencias del personal, porque claramente cada quien tiene las suyas para aportar desde cualquiera de los ambientes.

Leonardo Latorre P.

En un libro reciente del profesor Jeimy J. Cano[1] leí que, lo primero que se debe tener en cuenta para poder cerrar la brecha entre TI y TO, es que los profesionales de cada especialidad deben conocer el negocio. En ocasiones, las personas de TI se dedican solamente a lo suyo, pero no saben cuál es el *core* de su negocio. Así mismo, esto funciona para los profesionales de TO, aunque en algunas oportunidades estos últimos conocen un poco más del proceso para el cual están trabajando. También es necesario hacer unas auditorías y análisis de riesgos conjuntos entre TI y TO para verificar las brechas existentes en seguridad y mediciones que permitan definir estrategias conjuntas.

Felipe Silgado Q.

En términos de la visión, los asuntos son muy independientes entre TI y TO y pueden tender a la convergencia en términos de procesos de tecnologías y equipos de personas. Hoy en día existe mucha diferencia en empresas del sector industrial, de energía, de gas, las cuales funcionan de otra forma y están muy marcadas las características de TI, frente a las de TO. No obstante, con la evolución de la misma tecnología y los sistemas existentes relacionados con virtualización y plataformas más abiertas, ya no son tan cerrados. Sistemas basados, por ejemplo, en Linux con equipos de control para operar en ese ambiente, lo que permite que sea posible administrar desde un punto centralizado a nivel de procesos. En cuanto a las personas también sucede lo mismo. En la aplicación es donde puede observarse una diferencia que requiere una especialización en el equipo de trabajo, porque cualquier persona no puede operar equipos específicos, para lo que se requieren experiencia y conocimiento, además de la claridad del negocio. Existen muchas compañías en las que se busca un cambio para tener una sola área de tecnología, de manera

[1] Cano, J. (2016) *Manual de un CISO. Reflexiones no convencionales sobre la gerencia de la seguridad de la información en un mundo volátil, incierto, complejo y ambiguo*. Bogotá, Colombia: Ediciones de la U.

de evitar el funcionamiento de dos islas separadas y sin comunicación entre ellas, con miras a aprovechar el conocimiento que tienen los profesionales de cada uno de esos dos equipos. Es necesaria la sinergia de la administración y la operación de tecnologías de información para que el negocio funcione mejor. En las industrias que utilizan equipos de control para su funcionamiento, desarrollo y cumplimiento de sus objetivos, seguramente ese tema tarde o temprano llegará. El sector financiero está muy a la vanguardia en *robotics* y es una tendencia que funciona para ambos ambientes de TI y TO.

Diego Andrés Zuluaga U.
Para la construcción de una vista conjunta, se debe partir de un sistema de gestión de seguridad y ciberseguridad integrado entre TI y TO, que reconoce las diferencias de los entornos y las incorpora, incluyendo las excepciones que existen. Por ejemplo, los asuntos relacionados con el parchado y el cambio de los entornos. Entendiendo el sistema de gestión como una mejora continua.

Jeimy J. Cano M.
Cuando se va a hacer un sistema de gestión integrado ¿habría que cambiar el lenguaje?

Diego Andrés Zuluaga U.
Desde mi experiencia consideramos activos y ciberactivos, pero se usan indistintamente, entendiendo que los activos de información tienen su origen en los datos e información y su clasificación es en confidencialidad, integridad y disponibilidad; y, los ciberactivos, también se pueden clasificar en estos criterios, pero se refieren más a los sistemas que mantienen la operación confiable de los activos que controlan o soportan. Se trata de considerar que las tecnologías usadas en la operación y de las cuales dependen los activos críticos, requieren unos niveles de confidencialidad, integridad y disponibilidad solicitados por el responsable y son garantizados por el custodio. En últimas, un sistema de gestión se puede lograr en forma similar, entendiendo que el objeto de protección puede ser o la información misma u otros activos reconocidos en las normas como los de *hardware* y *software*, en el contexto de las TO son los activos que controlan los procesos industriales. Es necesario homologar lenguaje, tener en cuenta que, si se les llega a las personas de operación con la puesta en marcha de un sistema de gestión de seguridad de información basado en ISO 27000, se van a preocupar. Pero si se van incluyendo las excepciones basadas en riesgo y reconociendo las diferencias del entorno, se logra hacer un sistema de gestión para mejorar. También considero conveniente la creación de una nueva arquitectura unificada y complementaria, que lleve a la defensa en profundidad hacia esas zonas del perímetro interno que tenemos que construir, con perímetros de seguridad cada

vez más internos, que lleguen a las zonas en donde están las tecnologías de operación, con toda la calma, estudio y pruebas que eso requiere. Por último, llegar al *hardening* continuo que puede ser uno de los puntos más riesgosos. Todo esto enmarcado en un aprendizaje cruzado, entendiendo que el otro también tiene la razón. En otras palabras, las personas de operación cuando se asustan en todo su derecho, tienen que transferir su susto a las personas de ciberseguridad, por ejemplo; y éstos a su vez deben escuchar muy bien para entrar en sintonía en la búsqueda de soluciones con base en sus necesidades reales y no en las que TI determine. Ese aspecto es clave del cambio, en la medida en que no se puede llegar con seguridad a la operación, pensando que TI determine cómo se debe operar.

Felipe Silgado
En este caso es importante lograr un lenguaje común para facilitar la comunicación entre los diferentes equipos de la organización. A nivel de seguridad y ciberseguridad, se manejan algunos conceptos que cambian, sobre todo desde el alcance de los dos temas; sin embargo, entre TI y TO es importante unificar el lenguaje para no generar puntos de discrepancia y que los roles y alcances de cada uno sean claros para toda la organización.

Sara Gallardo M.
Editora Revista Sistemas
¿Quién es la persona que debe ejercer el liderazgo para lograr el intercambio de aprendizaje y la puesta en marcha de acciones orientadas al funcionamiento mancomunado de TI y de TO, en dirección a lograr los objetivos del negocio?

Diego Andrés Zuluaga U.
Esa es una pregunta muy interesante. En el mundo ya se está logrando la convergencia en gestión de TI y TO, porque las tecnologías de operación se han visto permeadas por tecnologías de información, y cada vez más pueden ser administradas por personas del área de TI, para que las personas de operación puedan dedicarse más al *software* y a las características propias de la operación, sistemas de control industrial en general y a la parte ciberfísica, como los sensores, actuadores e inteligencia de nivel 1, entre otras funciones. Desde el punto de vista de seguridad, considero que el Oficial de Seguridad de la Información (CISO) debe asumir esa complejidad y no hay cómo quitársela. Pero, aclaro que debería existir una persona que lo apoye en todos los temas relacionados con ciberseguridad industrial, porque es quien puede dedicarse a entender ese mundo de una manera mucho más fuerte, para balancear las necesidades de seguridad administrativas con las de operación. En resumen, como en general en seguridad, son asuntos de personas, tecnologías y procesos, en los que las personas deben lograr el aprendizaje continuo y

en cuanto a las tecnologías, la arquitectura y los procesos establecer un sistema de gestión que evolucione.

Wilmer Prieto G.
Es necesario considerar cuáles son los marcos de referencia internacionales con cierto nivel de madurez para tomar lo mejor de los dos mundos en el ecosistema de ciberseguridad a nivel nacional. Debemos basar los esfuerzos en identificar modelos o marcos de referencia que puedan ser moldeados hacia las realidades de nuestro país. No se trata de hacer "copy, paste" para volverlo una norma técnica colombiana y establecerlo como una camisa de fuerza. Por el contrario, se deben buscar las referencias para crear lo que yo denomino "la camisa a la medida" para la organización. Es necesario enfocarse en el ciber-riesgo de manera que sea transversal para los desarrollos.

Jeimy J. Cano M.
En el tema de seguridad industrial el riesgo y ciber-riesgo es otra distinción que se debe hacer. ¿Es así?

Wilmer Prieto G.
Es necesario aprovechar lo que ya está hecho y funciona muy bien.

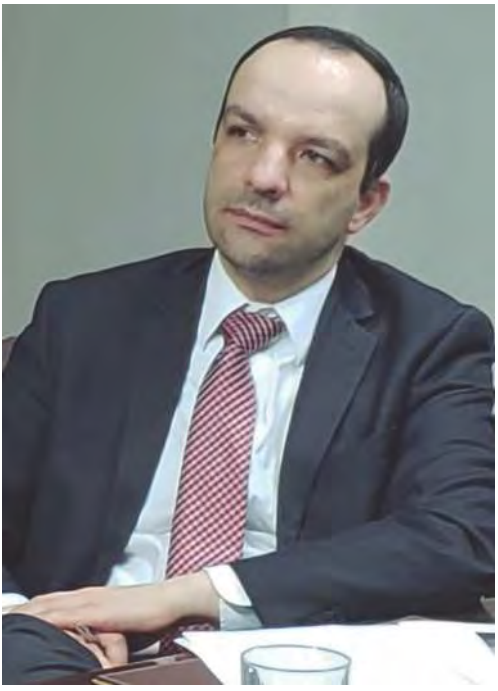
Diego Andrés Zuluaga U.
Estoy de acuerdo en que es necesario aprovechar lo que funciona bien y lo que más le preocupa al personal relacionado con la TO, es decir, los riesgos de las personas, de los equipos, del medio ambiente. Se trata de advertirles sobre el nuevo actor en ese panorama de riesgo para evitar cualquier tipo de impacto, un *hacker* que puede causar daño. Enfatizarles sobre la veracidad del riesgo, con ejemplos concretos, como los apagones en Ucrania, hornos de producción de acero apagados, *ransomware* en sistemas industriales, ataques a equipos de *safety,* entre otros de los eventos sucedidos en el mundo. De esa forma se toman los lenguajes de riesgos conocidos para sumarles una amenaza adicional, que permita identificar si podría causar un daño real. Cuando ellos entienden la dimensión del asunto actúan apoyando los proyectos de ciberseguridad industrial.

El tema del ciber-riesgo no solamente hay que llevarlo en términos organizacionales, sino a nivel nacional para poder definir estrategias acordes con los riesgos cibernéticos y pasar de lo cualitativo a lo cuantitativo para hacerlo medible y comparable, lo cual hoy no es posible, porque no se registran siempre de la misma manera entre empresas y menos entre sectores. Se debe medir la eficiencia de los programas y para ello es necesario determinar, adaptar y usar las mejores metodologías en gestión de riesgo. El Gobierno, a través del Ministerio de Tecnologías de la Información y Comunicaciones (Mintic), está desarrollando esfuerzos en el modelo de riesgos de seguridad digital, dentro de las acciones derivadas

del Consejo Nacional de Política Económica y Social (CONPES) 3854 y en el sector eléctrico, desde el Consejo Nacional de Operación se han desarrollado guías de primer nivel basadas en escenarios claves de riesgo.

Un marco de mejora continua también es muy importante y en esto la homologación del lenguaje es fundamental. Por otra parte, encontrar un modelo de riesgos que nos permita identificar, proteger, detectar, responder y recuperar logrando esa resiliencia dentro de los entornos cibernéticos, para innovar y homologar.

Felipe Silgado



Desde el punto de vista de riesgo y ciber-riesgo, los escenarios en ambos casos son diferentes y, por ende, deben ser abordados de forma distinta. Sin embargo, existen marcos ya definidos para gestión de riesgo y ciber-riesgo como la ISO 31000, ISO 27005, la guía para realizar valoración de riesgos del NIST (800-30) entre otros, que sirven como base para las organizaciones.

Jeimy J. Cano M.

¿Existen prácticas de seguridad convergente entre TI y TO? ¿Qué prácticas o referentes se usan hoy?

Juan Mario Posada D.

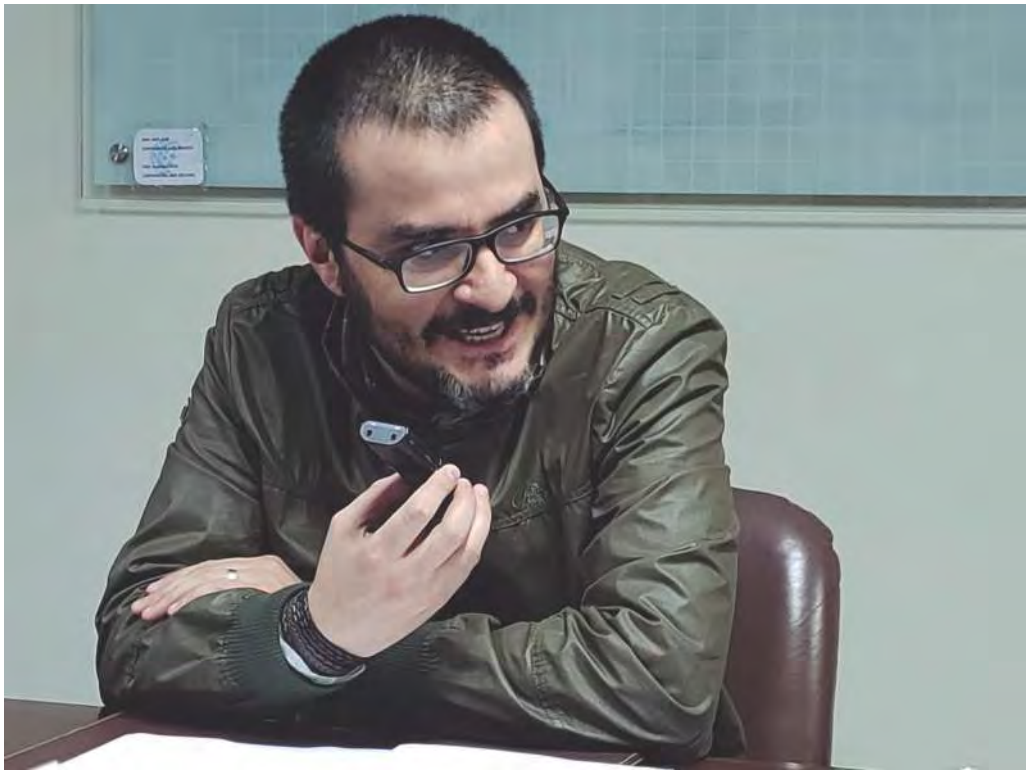
Es absolutamente indispensable lograr la empatía entre los dos mundos. Coincido en esa búsqueda, es decir “ponernos en los zapa-

tos del otro", para que las personas de TO puedan entender que TI lo que busca es fortalecer su entorno tecnológico. Los dos mundos hoy tienen la preocupación viva en tal sentido. Tienen un objetivo común y, con seguridad, lograrán encontrar las soluciones requeridas. Obtener un sistema de seguridad en TO, lo más maduro que encontramos son las disposiciones de NERC CIP, IEC 62443, el Framework de Ciberseguridad de NIST o lo sugerido en el estándar ISO 27019.

Leonardo Latorre P.
Entre las principales prácticas o referentes usados hoy en TI encontramos la "ISO 27001", en TO se pueden destacar "IEC-62443", "ISA99" y "NIST SP800-82", además de los existentes para cada tipo de industria, como lo es el "API-1164" para la industria petrolera o el "NERC CIP-002 CIP-014" para la industria eléctrica. En términos de convergencia, el estándar IEC-62443, en sus nuevas revisiones, ha empezado a involucrar a fabricantes de TI y TO con el fin de asegurar la seguridad desde las etapas de diseño de productos y proyectos.

Jeimy J. Cano M.
¿Y existe la voluntad entre las partes para lograr ese trabajo y entendimiento conjuntos?

Diego Andrés Zuluaga U.
Una vista conjunta está relaciona-



da con la voluntad y hay que crearla. Existen algunos casos exitosos, dependiendo de cada sector. Esto requiere trabajar en la empatía y en la confianza, así como en generar valor para la operación con la seguridad. Las personas de TO han entendido que requieren disponibilidad y que la operación sea adecuada y este es un atributo clave de la seguridad. Prevenir, por ejemplo, un *ransomware*. Se trata entonces de aportarle a la operación, así evitamos que se deba parar la planta por no poder controlarla o tener que reinstalar todo, lo cual puede generar bastante tiempo de indisponibilidad. La seguridad además, busca monitorear y conocer el tráfico de red, con lo cual se pueden detectar anomalías que indicarían equipos en falla o similares aportando a la operación y no sólo a determinar la amenazas.

Felipe Silgado

Desde mi punto de vista el tema aquí se vuelve algo político dentro de la organización, dado que generalmente estas áreas de TI y TO se encuentran dentro de equipos diferentes. Sin embargo, tratando la cultura de la organización y sensibilizando a todos los equipos responsables, iniciando por la alta gerencia, se puede lograr que haya un trabajo real en equipo.

Wilmer Prieto G.

En mi opinión, se trata más de un asunto político que de voluntad. Entre el área tecnológica y la de negocio la diferencia es sustancial y existe el juzgamiento entre ellas, lo que conduce más a la discordia que a un beneficio. Se trata de sensibilizar para entender la problemática, de manera de asumir posiciones conjuntas de cara a las amenazas que, al final, no es otro asunto que cultura, que parte de la alta dirección hacia todos los niveles de la organización.

Diego Andrés Zuluaga U.

Lo que está sucediendo con los sistemas de control industrial ya había pasado. Recuerdo a finales de los 90, cuando dictaba una charla denominada "*Hacker*, realidad o ficción", para que las personas dentro de la empresa entendieran que era una posibilidad, que podía pasar. En esa época no existía el miedo, apenas se iniciaban las conexiones a Internet; en alguna universidad se tenía una dirección IP pública para cada equipo en la red. Era la confianza en un mundo por el que se transitaba hacia un barrio que no conocíamos y que creíamos bue-

no. Después fue que nos dimos cuenta de que el barrio era diferente. Esa misma experiencia hay que ponerla "sobre la mesa" ahora, para indicar que ese barrio es complicado. Es un proceso que toma mucho tiempo, alrededor del cual hay que sembrar confianza y lograr esto puede requerir esfuerzos de mediano y largo plazo.

Juan Mario Posada D.

Me llama mucho la atención que continuemos hablando de cultura; en el marco de un análisis cuidadoso, es tal vez la deuda más grande que tenemos en el mundo, sobre la seguridad en TI. Todavía encontramos personas que abren en forma indiscriminada correos cuyo origen no es verificado. Como parte de mi trabajo hacemos muchísimas pruebas de intrusión y dentro de éstas incluimos pruebas de ingeniería social, utilizando *phising* por correo electrónico, llamadas telefónicas, recorridos por las oficinas. Como resultado de ellas, seguimos encontrando en los escritorios información confidencial, respuestas a correos falsos, en los que las personas dan sus credenciales de autenticación, por ejemplo. De manera que soy enfático en señalar la cultura como el principal elemento en seguridad de la información. Y esto sucede porque no hemos logrado transmitir el mensaje en forma adecuada para gestionar el riesgo y actuar conforme a las necesidades de protección que se exige alrededor de los activos de información.

Leonardo Latorre P.

La sensibilización y la cultura son claves en la convergencia entre TI y TO. Con base en la experiencia propia, puedo concluir que concienciar a las personas de operación conocedoras del proceso, a los profesionales de TI y TO, y a las altas directivas de la empresa puede tener un mayor impacto en la seguridad, que la adopción de nuevos elementos dentro de la infraestructura tecnológica. Un habilitador fuerte para lograr esa voluntad en todos los niveles de la organización, no es otro que la sensibilización.

Wilmer Prieto G.

Quienes venimos trabajando estos asuntos desde hace tiempo, reconocemos que la palabra concienciación se nos quedó corta en materia de seguridad. De manera que es inminente el cambio de *awareness* por cultura y la sensibilización es la base para generarla. Quien es

culto toma los controles de una forma natural y se protege. Esto viene apoyando un concepto antiguo en materia de seguridad, denominado *firewall* humano. No es sólo hacer y decir, sino actuar de forma segura. Otro aspecto es el político, convertido en reto dentro de una organización. La empatía, la estandarización y la voluntad también son aspectos aquí mencionados y, al respecto, me pregunto ¿qué nos está pasando en Colombia que no sucede a nivel mundial? Y es que la academia ayuda a formar ingenieros, pero también debe preocuparse por la formación de líderes que sepan de TI y TO, de una forma integral, con conocimientos sobre comunicaciones y finanzas, entre otros asuntos. Y es cuando surge la voluntad, para ser un líder formal o informal dentro de la organización. Las personas no deben esperar a tener un cargo directivo o gerencial para ejercer liderazgo. Es necesario permear en forma horizontal y transversal dentro de una empresa. El área de seguridad es un habilitador del cambio, visionaria para considerar el futuro de la seguridad y prepararse para ese futuro. Es necesario saber vender nuestras ideas, casos de negocio, casos de uso y manejar la comunicación en tiempos de crisis. Y otro aspecto muy importante es la investigación, de la cual adolecemos tanto en el país. Traemos tecnologías, marcos de referencia, conocimiento internacional, pero desarrollamos muy poco en Colombia. Walter Isaacson, biógrafo de Steve Jobs, señaló que las economías fuertes del siglo XXI son aquellas que tienen un equilibrio entre las humanidades y las ciencias y dentro de éstas se encuentra la tecnología. Estamos viviendo la revolución digital y es necesario aprovechar este punto de quiebre para generar conocimiento, con el propósito de acortar la brecha con los países denominados primer mundistas. El reto es transversal, en todas las verticales de negocios, en materia de educación, y en la sociedad.

Jeimy J. Cano M.

¿Cómo construir una seguridad convergente entre TI y TO? ¿Qué elementos debería tener? ¿Es un reto de lenguaje? ¿De estándares?

Juan Mario Posada D.

El tema de los referentes de estándares internacionales es un asunto muy importante. Soy enemigo de reinventar la rueda, pero sí considero relevantes las adaptaciones de cada elemento a la realidad de cada empresa. Cobit e ISO 27001 son válidos siempre que se puedan adaptar a las circunstancias de TO, y no pueden ser la tarjeta de presentación para sensibilizar a un profesional de planta. La industria de automatización también es consciente de tales circunstancias y ha empezado a generar estándares como el caso de ISA, organización en la que gran número de profesionales de la automatización se reúne para determinar la forma en que van a abordar la seguridad y la

ciberseguridad de cara a TO. La ruta a la convergencia es una realidad, pero lo cierto es que en un gran volumen apenas empiezan su camino hacia allá. Y enfatizo en la necesidad de la comunicación, a través de un lenguaje entendible para la alta dirección y el resto de las personas de cualquier organización. De ahí que los CISO tenemos la obligación de propender por un ejercicio integral, debemos ser políglotas, hablar el lenguaje claro para todos, para poder transmitir el conocimiento sobre los asuntos que hemos venido mencionando.

Felipe Silgado Q.
En Colombia todavía adolecemos en muchos sentidos de aspectos que tienen que ver con seguridad. Uno de ellos, la investigación. No obstante, el trabajo de las mesas de infraestructura crítica del Comando Conjunto Cibernético (CCOC) y la misma academia son espacios que sirven de punto de partida para adquirir conocimiento y crear relacionamiento en el sector. La convergencia se da cuando existen la cultura y el conocimiento. En el mercado existen muchos profesionales con buenos conocimientos sobre TI, pero en lo relacionado con TO no sucede lo mismo. La nueva generación de estudiantes será la que llegue con todos los elementos para ejercer en una forma integral, para que se dé la convergencia. Como país nos diferenciamos de la cultura norteamericana y europea y adoptamos las tecnologías desarrolladas en esos entornos diferentes al nuestro, lo que produce sus efectos en términos de tales diferencias culturales. Nuestra idiosincrasia dificulta la convergencia. La evolución tecnológica, aunque registra avances, también sufre de carencias. No tenemos los suficientes profesionales, ingenieros de Sistemas, y esto genera una problemática que se debe atender.

Leonardo Latorre P.
No es un reto de lenguaje o de estándares; sin embargo, es importante que cada negocio o industria use los referentes que existen actualmente como guía para construcción de su propio modelo de seguridad, comprometiéndose en que cada profesional de TI o TO que participe en esta construcción entienda el negocio que soportan las TI y TO. Y partiendo del desarrollo de auditorías y análisis de riesgos conjuntos entre TI y TO para verificar las brechas existentes en seguridad y mediciones que permitan definir estrategias conjuntas

Jeimy J. Cano M.
Ante lo aquí expuesto, alguien tiene que ceder y, desde esa perspectiva ¿qué es lo más fácil: que lo haga TI o TO?

Felipe Silgado Q.
En mi opinión, es más fácil entre las personas de TI que entre las de TO, debido a que las primeras están del lado del negocio y, al percibir cualquier posible impacto, es más difícil que lleguen a ceder. Sin

embargo –como ya lo mencioné-, es importante trabajar desde la alta gerencia para generar cultura en la organización, buscando sinergia entre los equipos para lograr colaboración mutua.

Diego Andrés Zuluaga U.
Es necesario basarse en un sistema de gestión de seguridad integrado, considerando las particularidades del ambiente TO. Es necesario ir desarrollando las capacidades claves para lograr niveles de madurez. En todo desarrollo de cultura se atraviesa por tres fases: comunicación, acompañamiento y control. En algunos niveles de infraestructura crítica ya se han recorrido tales fases.

En términos de prácticas de seguridad convergentes, a mí me gusta el NIST cibersecurity framework, que puede aportar a los dos ambientes, es aceptado por ambos y es un marco general inicial. Las normas ISO 27000 forman el sistema de gestión y habrá normas para cada entorno, podemos considerar la ISA/IEC 62443 y el documento de Guía para la Construcción de un Sistema de Gestión de la Ciberseguridad Industrial del Centro de Ciberseguridad Industrial para la TO. En resumen, todas las normas son mapeables entre sí y podemos aprovechar esto para usar las capacidades existentes y desarrollarlas hacia las necesidades específicas de la organización.

Wilmer Prieto G.
En la medida en que empleemos marcos de referencia desarrollados específicamente para los retos que enfrenta la ciberseguridad como, por ejemplo, NIST Cybersecurity Framework, podremos encontrar un sano equilibrio entre TI y TO, pero siempre, la decisión de inclinar la balanza está en el beneficio para el negocio, y recordemos que en este tipo de entornos TO es el *core* del negocio.

Leonardo Latorre P.
Es más fácil que TI ceda hacia TO, entendiendo que muchos de los profesionales que trabajan en el desarrollo de prácticas y estándares de TO son profesionales educados en TI y con experiencia en TO.

Sara Gallardo M. *Periodista comunicadora, universidad Jorge Tadeo Lozano. Ha sido directora de las revistas Uno y Cero, Gestión empresarial 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; de los diarios La Prensa de Panamá y La Prensa Gráfica de El Salvador y corresponsal de la revista IN de Lanchile e investigadora en publicaciones culturales. Se ha desempeñado también como gerente de Comunicaciones y Servicio al Comensal en Inmaculada Guadalupe y amigos en Cía. S.A. (Andrés Carne de Res); es editora de esta revista.*