No. 147 Abril - Junio 2018 DOI: 10.29236/sistemas ISSN 0120-5919

SISTEMAS

Tarifa Postal Reducida Servicios Postales Nacional S.A. No. 2015-186-4-72, vence 31 de Dic. 2018

Profesionales en seguridad de la información:

¿evolución o revolución?

ACIS
ASOCIACIÓN COLOMBIANA DE INGENIEROS DE SISTEMAS
Calle 93 No. 13 - 32 of. 102
Bogotá, D.C.
www.acis.org.co

Deloitte.

Decisiones estratégicas para desafíos complejos

Auditoría, Impuestos, Asesoramiento Financiero, Consultoría y Outsourcing.

www.deloitte.com/co | cmercadeo@deloitte.com

En esta edición

Editorial 4

Una mirada a los profesionales en seguridad de la información
DOI: 10.29236/sistemas.n147a1
¿Cómo es el perfil actual de los profesionales en seguridad de la información? ¿En qué ha cambiado? ¿Se observa evolución? ¿Se registra una revolución?

Columnista Invitado 8

Evolución del profesional en Seguridad de la Información ante la revolución tecnológica
DOI: 10.29236/sistemas.n147a2
Los retos de los profesionales y las organizaciones en su búsqueda para ocupar los cargos, desde los niveles estratégicos hasta los técnicos y operacionales.

Entrevista 14

Malcolm Harkins: una visión global
DOI: 10.29236/sistemas.n147a3
Reconocido líder en seguridad de la información a nivel internacional compartió su amplia experiencia.

Investigación 16

XVIII Encuesta Nacional de Seguridad Informática
Evolución del perfil del profesional de Seguridad Digital
DOI: 10.29236/sistemas.n147a4
La encuesta nacional de seguridad informática, capítulo Colombia, soportada por la Asociación Colombiana de Ingeniero de Sistemas (ACIS) y realizada a través de Internet, entre los meses de febrero y abril de 2018, contó con la participación de 234 encuestados, quienes con sus respuestas permiten conocer la realidad del país.

Cara y Sello 43

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.

Uno 65

El profesional de seguridad de la información. Un análisis de su evolución: 1960-2030+
DOI: 10.29236/sistemas.n147a6
La rápida evolución del entorno de negocios y el advenimiento de otra revolución industrial revelan nuevos retos para el área de seguridad de la información. En este sentido, analizar el desarrollo de esta área a lo largo del tiempo, permite observar los desafíos para los profesionales de seguridad de la información en un contexto gobernado por la inestabilidad y la incertidumbre. Por tanto, este documento busca reflexionar sobre las variaciones en sus competencias y proyectar el ejercicio de una práctica de protección, consolidada con los requerimientos de las organizaciones y los negocios del siglo XXI.

Publicación de la Asociación Colombiana de Ingenieros de Sistemas (ACIS)
Resolución No. 003983 del Ministerio de Gobierno
Tarifa Postal Reducida Servicios Postales Nacional S.A. No. 2015-186 4-72
ISSN 0120-5919
Apartado Aéreo No. 94334
Bogotá D.C., Colombia

Abril - Junio 2018
Calle 93 No.13-32 Of. 102
Teléfonos 616 1407 – 616 1409
A.A. 94334
Bogotá D.C.
www.acis.org.co

Una mirada a los profesionales en seguridad de la información

DOI: 10.29236/sistemas.n147a1

¿Cómo es el perfil actual de los profesionales en seguridad de la información? ¿En qué ha cambiado? ¿Se observa evolución? ¿Se registra una revolución?

Jeimy J. Cano M.

En un escenario de disrupciones digitales, de cambios acelerados e innovaciones emergentes, en el que las organizaciones adelantan acciones para dar cuenta de una nueva transformación digital, la seguridad de la información se encuentra en un proceso de reinvención, con el fin de atender los retos emergentes que supone acompañar a las organizaciones para articular su promesa de valor con las exigencias de un entorno digital y tecnológicamente modificado.

En consecuencia, los profesionales de seguridad de la información, deben comprender que es necesario revisar los paradigmas de protección y control que han aprendido, para repensarlos a la luz de la dinámica que impone un escenario digital y dinámico como el actual. Esto es, las consideraciones tradicionales de control de acceso se deben conjugar con las emergentes relativas al control de uso, para balancear la necesidad de agilidad del negocio, con la confianza digital que los clientes requieren para conectarse con el producto y/o servicio de la empresa.

Considerando lo anterior, la Revista Sistemas ha dedicado su número 147 para reflexionar sobre la evolución de los profesionales de seguridad de la información, con el fin de establecer algunos puntos de referencia y concretar algunos análisis que permitan ver cómo podrían ser la evolución y los retos de los profesionales en la protección de la información, en el escenario de la cuarta revolución industrial.

En primer lugar, nuestro columnista invitado aborda la evolución del profesional en seguridad de la información frente a la nueva revolución industrial. Se refiere a sus retos para ocupar los cargos y ejercer la profesión, en la que una formación integral es clave para vincularlos en niveles estratégicos, técnicos y operacionales. Para entrar en contexto, inicia su análisis describiendo el marco histórico de estos asuntos, hasta los atributos que la realidad del momento exige a dichos profesionales, perfil que va más allá del título obtenido.

El entrevistado en esta edición es Malcolm Harkins, un líder reconocido a nivel internacional en seguridad de la información. Economista especializado en el tema que nos ocupa, conocedor de la dinámica empresarial y la protección del valor de las empresas, quien fue directivo de Intel Corp. durante 23 años. La conversación en vivo y en directo con este profesional portador de varios premios y autor de artículos y un libro con dos ediciones, está publicada en el portal de esta Asociación (http://www.acis.org.co), en el espacio dedicado a la revista Sistemas.

La investigación que anualmente se realiza sobre el estado de la seguridad de la información en Colombia, que este año llega a su edición número 18, muestra una evolución de las prácticas de seguridad y control en el país, un reconocimiento del papel del ejecutivo de seguridad y las tensiones emergentes frente al entorno digital y tecnológicamente modificado.

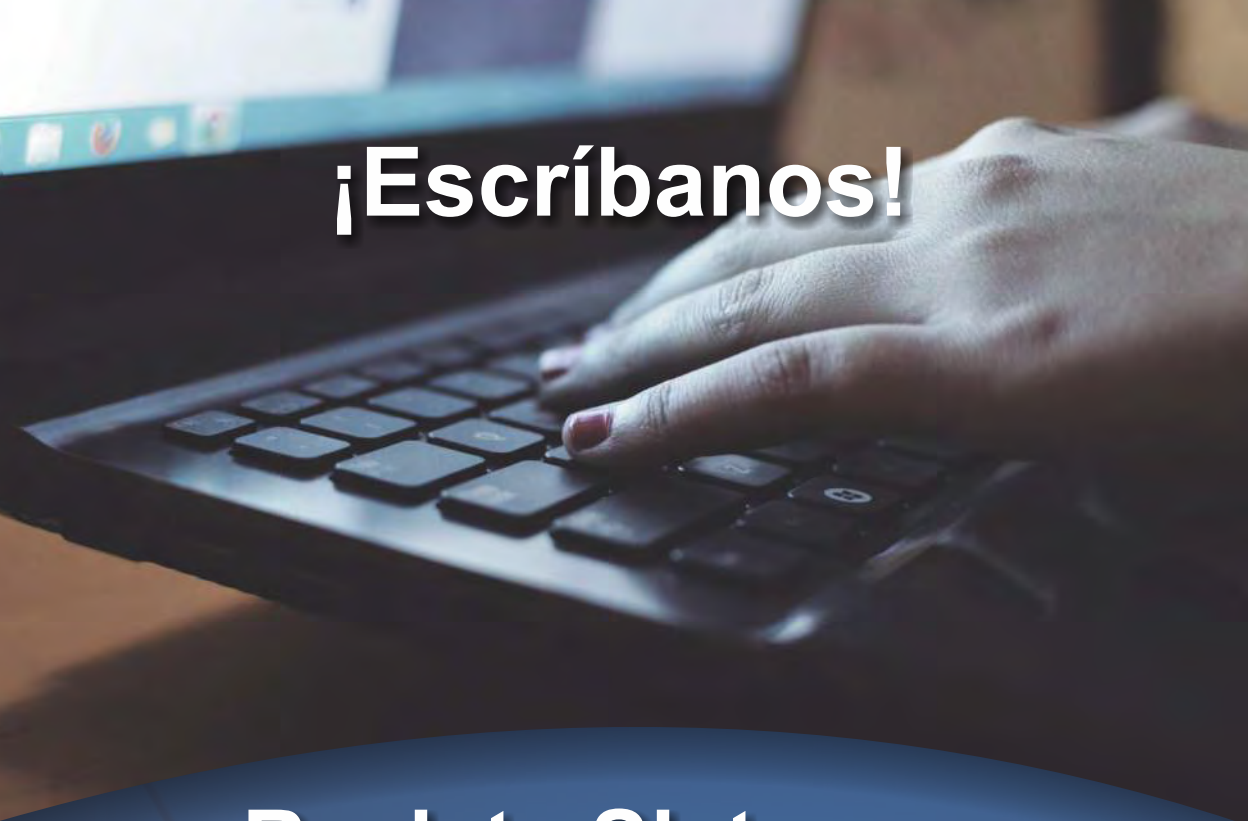
Para el tradicional debate en la sección Cara y Sello, reunimos a importantes profesionales de diferentes entidades, con el propósito de analizar la ciberseguridad industrial, la seguridad de la información y el negocio, en términos de encuentro o divorcio entre tales am-

bientes. Este diálogo puso sobre la mesa las diferentes tensiones existentes relacionadas con la convergencia de la seguridad, entre los ambientes de tecnología de operaciones y de tecnología de información.

Finaliza el contenido con el análisis de la evolución del profesional de seguridad de la información desde 1960, con una visión futurista más allá del 2030. Mirada que contempla sus retos en medio de la inestabilidad y la incertidumbre que gobiernan el ambiente. Este artículo advierte las variaciones en sus competencias y las prácticas de protección, diseñadas con base en los requerimientos de las organizaciones y de los negocios en este siglo XXI.

Si bien hay mucho por revisar y analizar frente a la evolución de los profesionales de seguridad de la información en esta nueva era digital, este número busca motivar algunas reflexiones académicas y prácticas para continuar explorando posibles futuros, para concretar acciones que forjen la nueva generación de analistas y ejecutivos que custodien la promesa de valor en las empresas del nuevo milenio.

***Jeimy J. Cano M., Ph.D, CFE**. Profesor Asociado. Escuela de Administración, Universidad del Rosario. Ingeniero y Magíster en Ingeniería de Sistemas y Computación de la Universidad de los Andes. Especialista en Derecho Disciplinario de la Universidad Externado de Colombia. Ph.D in Business Administration por Newport University, CA. USA. Profesional certificado como Certified Fraud Examiner (CFE), por la Association of Certified Fraud Examiners. Director de la Revista Sistemas de la Asociación Colombiana de Ingenieros de Sistemas –ACIS–.*



¡Escríbanos!

Revista Sistemas

Asociación Colombiana de Ingenieros de Sistemas (ACIS)

Diríjase a la editora de la revista:
Sara Gallardo M.
saragallardo@acis.org.co

ACIS
ASOCIACIÓN COLOMBIANA DE INGENIEROS DE SISTEMAS

Calle 93 No. 13 - 32 of. 102
Bogotá, D.C.
www.acis.org.co

Evolución del profesional en Seguridad de la Información ante la revolución tecnológica

DOI: 10.29236/sistemas.n147a2

Los retos de los profesionales y las organizaciones en su búsqueda para ocupar los cargos, desde los niveles estratégicos hasta los técnicos y operacionales.

Yezid E. Donoso Meisel

La evolución de la seguridad de la información, desde sus diferentes aristas (tecnología, metodologías, procesos, experticia, conocimiento, investigación, innovación, entre otros) ha estado ligada a la misma evolución de la humanidad. Revisando la historia, podemos observar que las civilizaciones, resguardaban su información como un tesoro de vital importancia; en particular, lo asociado a los ámbitos de

defensa de sus Estados ante confrontaciones militares y, también, en lo referente a los aspectos económicos y políticos.

Cuando la humanidad y las civilizaciones ingresaron a la era de las comunicaciones análogas y posteriormente digitales, empezó una nueva etapa en la evolución de la seguridad de la información, con la diferencia de que, en esos momentos, se manifestaba a través de una serie de señales electromagnéticas. Para los expertos en temas de seguridad de la información fue un reto entender estas tecnologías para definir nuevas estrategias y los aspectos técnicos, encaminados a salvaguardar el valor intrínseco que la información podría tener para la sociedad o para un Estado.

Como ejemplo, podemos mencionar la máquina que diseño e implementó Alan Turing y su equipo de trabajo, cuya proyección generó las bases de la computación. En plena segunda guerra mundial, la Gran Bretaña no tenía militarmente ventaja competitiva, con respecto a la Alemania Nazi. Por esta razón, es que un grupo de expertos criptógrafos tuvo la fabulosa idea enfrentar el desafío con mejor tecnología ("La Máquina de Turing"), para descifrar los códigos transmitidos por la máquina alemana "Enigma".

Posteriormente, llegó el desarrollo de la revolución Digital y con esta, el crecimiento exponencial de tecnologías y de la mano, los nuevos riesgos digitales y riesgos en el ciberespacio. Al respecto, solo para ejemplificar, podemos encontrar nuevas tecnologías llamadas emergentes, tales como: -IoE- Internet of Everythings, Social Networks of the Things, 5G, Network Function Virtualization –NFV-, Softwarization, Cloudification, Machine-to-Machine Communications -M2M-, entre otras. O las nuevas tecnologías incipientes (BYOD – Bring Your Own Device, Internet of Things -Iot-, Smart Cities, Software Defined Networking -SDN-, Unmanned Aerial Vehicles –UAV-, Drones, Artificial Intelligence, FoG Computing, Industria 4.0) las cuales se encuentran todavía en una etapa inicial de desarrollo, pero han demostrado su potencial para cambiar las bases de la competición. Así mismo, todas aquellas tecnologías maduras: básicas y claves para las organizaciones (Cloud Computing, Big Data, Data Analytics, entre otras. Todas ellas han abierto un espectro de nuevos servicios y aplicaciones para las organizaciones y para la sociedad.

Debido a lo anterior y a los nuevos desarrollos tecnológicos que se avecinan, como ingenieros de sistemas y áreas afines, debemos comprender, asimilar y ser capaces de proyectar a las organizaciones, hacia ese mundo lleno de nuevos y cambiantes desafíos, a través del apalancamiento de las TIC, con el propósito inherente de mejorar la calidad de vida de los miembros de la sociedad.

Algunos análisis muestran aspectos relevantes de la seguridad de la información. Según "Hype Cycle for ICT in Latin America, 2017", informe de Gartner con fecha Julio 19 de 2017, se refiere a cómo la Arquitectura de Seguridad y Seguridad Digital se encuentran en el pico máximo de expectativas de aplicabilidad en las áreas de TI en Latinoamérica. Por otra parte, según "Hype Cycle for Digital Government Technology, 2017", informe de Gartner con la misma fecha de Julio de 2017, muestra al Blockchain en el pico máximo de expectativas de aplicabilidad, no solo en el sector gobierno sino en diferentes tipos de entidades. Adicionalmente, ambos documentos, muestran que el área de detección de fraudes en TI, se encuentra en su expresión máxima de la productividad. En este punto, podemos mencionar, que los análisis realizados por Gartner evidencian que no solo nuestro país necesita expertos en temas de seguridad de la información, sino en áreas de conocimiento y competencias específicas en el desarrollo profesional.

En estos momentos, considero muy ambicioso hablar sobre el experto en seguridad de la información, considerando los distintos frentes en esta área del conocimiento. Encontramos expertos en pruebas de seguridad, en delitos informáticos (aspectos legales y procedimentales), en seguridad de las comunicaciones, informáticos forenses, entre muchos otros, impactados en términos de competencias por las exigencias de esta revolución tecnológica.

Las condiciones registradas a través del tiempo frente a la seguridad de la información han dado lugar a que las organizaciones y los expertos entendieran que estos asuntos no sólo son técnicos, sino tácticos y estratégicos también para el Estado, a la hora de definir directrices a nivel nacional.

De ahí la necesidad de formar profesionales que entiendan el negocio (aspectos estratégicos y tácticos) para definir una arquitectura de solución y transición en seguridad de la información. En otras palabras, disponer de expertos en seguridad que puedan actuar en forma transversal y entre los altos niveles de dirección dentro de las organizaciones.

En ese contexto, surgen nuevos cargos, como el *Chief Information Security Officer* (CISO), profesional encargado de la toma de decisiones a nivel de seguridad de la información. En el nivel táctico, encontramos los arquitectos de seguridad, encargados de comprender las necesidades y retos del negocio, capaces de diseñar una arquitectura de integración entre los diferentes componentes tecnológicos, para suplir los requerimientos asociados a los riesgos relacionados con las TIC. En este nivel están los gerentes de operaciones de seguridad y los de continuidad de los

servicios de TI, profesionales responsables de liderar los proyectos encaminados a mantener la operación del negocio en forma segura, además de recuperar los servicios de infraestructura de TI, frente a un ataque informático. También figuran los consultores de seguridad, profesionales expertos en proporcionar las recomendaciones necesarias, preventivas como curativas, ante cualquier incidente.

En el nivel técnico está el analista de seguridad, cuya función principal es ejecutar las tareas operacionales del programa de seguridad de la información relacionadas con riesgos, vulnerabilidades, amenazas y controles técnicos, desde el punto de vista de la industria. Adicionalmente, su rol también contempla la implementación de las políticas de seguridad, estándares, procedimientos y guías que, algunas veces, incluye responsabilidades en la planeación y diseño de iniciativas de mejoramiento.

Por otra parte, su formación ha sufrido modificaciones toda vez que, a los programas con certificaciones de marcas comerciales, se suman los de pregrado enfocados en seguridad de la información, las maestrías e inclusive doctorados.

Para finalizar el análisis deseo referirme a un nuevo reto y es que no basta contratar un profesional con un título que demuestre su nivel de conocimiento y experiencia, sino una persona que reúna una serie de atributos –soft skills- adicionales, relacionados a continuación.

Visionario. Con habilidad para ver cómo los aspectos del programa completo de seguridad de la información serán observados y puestos en marcha.

Comandante/Comendador. Con capacidad para inspirar, motivar y liderar a otras personas. En otras palabras, un profesional calmado, reflexivo, analítico, un ejecutivo a quien se pueda recurrir en busca de una dirección.

Escritor. Capaz de comunicar las ideas y conceptos en una forma ordenada y estructurada.

Presentador. Con capacidad para formular ideas y conceptos, mediante una oralidad estructurada y clara.

Arquitecto. Este atributo provee la habilidad para ver el entorno de la organización de una forma integral y poder profundizar dentro de las características técnicas hasta donde sea necesario.

Consultor. Con habilidad para comprender los nuevos entornos y trabajar en una amplia variedad de proyectos e iniciativas.

Gurú (experto) técnico. Este experto ayuda a aclarar aspectos técnicos cuando existen discusiones respecto a su área de experticia. Este atributo requiere amplio cono-

cimiento en temas como sistemas operativos, redes, codificación de aplicaciones, bases de datos y seguridad de la información. Aunque no tiene un conocimiento profundo sobre cada tema, sí dispone de la comprensión de las interrelaciones entre diferentes tecnologías.

Educador. Se refiere a la persona con capacidades para enseñar y transmitir conceptos complejos de forma sencilla, que los usuarios más básicos puedan comprender y asimilar.

Cazatalentos. Un buen cazatalentos siempre mantendrá su mirada abierta analizando qué personas o recursos le podrán servir para cumplir sus metas. Este atributo puede ser muy útil durante los procesos de reclutamiento.

Vendedor. Con capacidad para mercadear y vender productos y servicios. Estos productos son típicamente una variedad de ideas, conceptos e iniciativas de su programa.

Planificador. Este atributo permite a las personas priorizar las acciones e iniciativas, coordinar la logística requerida para la ejecución en forma exitosa e identificar los recursos necesarios para la ejecución.

Negociador. Es la persona cuyo trabajo con los clientes, *stake holders* y equipos operativos consiste en ganar el soporte y apoyo para el programa de seguridad de la información y de sus respectivos proyectos e iniciativas.

Ejecutor. Logra que las cosas se realicen para su programa, mediante la comprensión de las diferentes políticas y aspectos operacionales.

Investigador. Responsable por mantener actualizadas las prácticas de seguridad, tendencias de la industria, nuevas características y otras áreas de conocimiento requeridas por el programa. Los investigadores logran estas metas a través del monitoreo de una variedad de fuentes de información internas y externas.

Auditor. Con habilidad para medir el estado actual de la seguridad dentro de la organización y evaluar el progreso.

Detallista. Persona orientada a observar los detalles para ayudar a crear una estructura que cumpla con un cierto nivel de estándar.

Organizador. Con habilidad para reunir, organizar, programar y coordinar grandes cantidades de información y recursos.

A continuación, se muestra un cruce sugerido por propuestas documentadas (Cuadro 1).

En conclusión, hoy las organizaciones requieren de profesionales expertos, con conocimientos y competencias muy particulares pa-

ra abordar los nuevos retos de la seguridad de la información en los diferentes niveles, de manera que las estrategias y tácticas puedan ser aplicadas y permear la empresa en forma transversal.

		Roles y Responsabilidades (Cargos)							
		CISO	Arquitecto de Seguridad	Consultor de Seguridad	Analista de Seguridad	Especialista para Formación	Gerente de Operaciones de Segurida	Gerente BCP / DR	Especialista Seguridad Física
Atributos	Visionario	X							
	Comendador	X	X				X	X	
	Escritor	X		X	X	X		X	
	Presentador	X	X	X	X	X		X	
	Arquitecto		X						X
	Consultor		X	X	X			X	
	Experto Técnico		X	X					
	Educador		X	X		X			
	Cazatalentos	X							
	Vendedor	X	X	X		X		X	
	Planificador	X				X		X	X
	Negociador	X	X	X			X		
	Ejecutor			X		X	X	X	X
	Investigador				X				
	Auditor						X		X
	Detallista						X	X	X
	Organizador	X			X	X			

Cuadro 1. Nota: Gentile, M., Collette, R., & August, T. (2006).

Referencias

Gentile, M., Collette, R., & August, T. (2006). *The CISO handbook : A practical guide to securing your company* . Boca Raton: Auerbach Publications.

Gartner (2017). Hype Cycle for ICT in Latin America (ID: G00328142).

Gartner (2017). Hype Cycle for Digital Government Technology. (ID: G0033 2564).

***Yezid E. Donoso Meisel**. Director Departamento de Ingeniería de Sistemas y Computación y Profesor Asociado, Universidad de los Andes. Ph.D (Cum Laude), Post PhD y D.E.A en Tecnologías de la Información, Universidad de Girona, España. Máster en Ingeniería de Sistemas Computación, Universidad de los Andes, Colombia. Ingeniero de Sistemas, Universidad del Norte, Barranquilla. Investigador Sénior Colciencias. Sénior Member IEEE. Presidente IEEE Colombia 2013-2014. Evaluador experto de la Comisión Europea. Tiene más de 150 artículos publicados en revistas internacionales indexadas, IEEE, ACM, IFIP y Conferencias Internacionales. Tiene cuatro libros publicados y ha recibido varios reconocimientos y premios nacionales e internacionales, incluyendo medallas otorgadas por el Ejército y la Policía Nacional de Colombia por sus aportes en el área de TI. Participa en varias juntas directivas de gremios en el área de TI.*

Malcolm Harkins: una visión global

DOI: 10.29236/sistemas.n147a3

Reconocido líder en seguridad de la información a nivel internacional compartió su amplia experiencia.

Sara Gallardo M.

"Un equipo no es un grupo de personas que trabajan juntas; un equipo es un grupo de personas que confía en el otro", es el principio que orienta el ejercicio profesional de Malcolm Harkins.

Licenciado en economía y un MBA en finanzas y contabilidad de la Universidad de California, es especialista en asuntos relacionados con la seguridad de la información, conocedor de la dinámica empresarial y la protección del valor de las empresas.

Uno de los recorridos más importantes lo hizo en Intel Corporation durante 23 años, empresa por la que transitó en línea ascendente y dejó huella en cada uno de los cargos ocupados, como CISO (Oficial de Jefe de Seguridad de la Información) hasta Vicepresidente y Director de Seguridad y privacidad (CSPO).

Es un profesional reconocido en el mundo de la seguridad como uno de los líderes en tecnologías de información y la industria "se lo pelea" como orador principal. Ha recibido infinidad de premios, reconocimientos y es autor del libro "Gestión del riesgo y seguridad de la información", además de coautor en la "Introducción a la Privacidad de TI".

En la actualidad es Jefe de Seguridad y Confianza (*Chief Security and Trust Officer*) en Cylance Corporation, empresa en la que le reporta al CEO y es el responsable del crecimiento del negocio, a través de una infraestructura confia-

ble de seguridad que contempla sistemas y procesos de negocios.

Su consagración profesional no limita sus actividades personales y administra muy bien el tiempo para disfrutar con la familia y los amigos al aire libre y compartir su afición por la buena mesa, aportando su propia sazón.

Conversamos ampliamente con Malcolm Harkins a través de una conferencia en línea que nuestros lectores podrán consultar en el siguiente enlace:

http://acis.org.co/revista147/content/entrevista-malcolm-harkins

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.*

XVIII Encuesta Nacional de Seguridad Informática

Evolución del perfil del profesional de seguridad digital

DOI: 10.29236/sistemas.n147a4

Resumen

La encuesta nacional de seguridad informática, capítulo Colombia, soportada por la Asociación Colombiana de Ingeniero de Sistemas (ACIS) y realizada a través de Internet, entre los meses de febrero y abril de 2018, contó con la participación de 234 encuestados, quienes con sus respuestas permiten conocer la realidad del país. La distribución se hizo a través de las diferentes redes sociales, comunidades y grupos, y contó con la cooperación de otras asociaciones como ISACA, Capítulo Bogotá, OWASP Capítulo Colombia, y CISOS.CLUB, entidades que colaboraron en dicho proceso para difundir entre sus diferentes grupos de interés el instrumento.

Este estudio cumple con varios propósitos. En primer lugar, muestra el panorama de las organizaciones colombianas frente a la seguridad de la

información y/o ciberseguridad, y su respuesta a las demandas del entorno actual. En segunda instancia, es un instrumento referente para Colombia y Latinoamérica, en la medida en que llama la atención de todos los sectores interesados en los temas relacionados con la seguridad.

La investigación refleja las opiniones de quienes contestan y el análisis está basado en la realidad representada en los datos obtenidos. En ese orden, lo primero que se hace para la obtención de los resultados es preparar y revisar las preguntas de la encuesta; acto seguido preparar los componentes tecnológicos necesarios, publicación e invitación al proceso, distribución a los grupos de interés y cooperantes, recepción de datos, cierre de la encuesta, validación de los datos, normalización y análisis, preparación del informe, preparación de la presentación y publicación de los mismos, en los diferentes medios dispuestos para ello.

Palabras clave
Seguridad de la información, encuesta, líder, perfil profesional, riesgos de información.

Andrés R. Almanza J.

Introducción

Entender la realidad nacional en materia de seguridad de la información y ciberseguridad, permite visualizar los retos a mediano y largo plazo, además de construir mejores posiciones al respecto en las organizaciones. Ese entendimiento sumado a conocer el contexto internacional, proporciona una proyección al entorno nacional para enfrentar los retos y desafíos en ambientes cada vez más permeados por la realidad digitalmente modificada.

De la misma manera que en otras versiones, la Encuesta Nacional pretende medir las dinámicas y lógicas de las empresas del país, ver otros referentes mundiales en la búsqueda y construcción de los propios.

Año tras año, este estudio ha reflejado cómo ha venido desarrollándose en Colombia la protección de la información en los entornos digitales y cómo en los diferentes sectores (industrial y empresarial), la seguridad y la resiliencia digital se convierten en un valor dentro de las organizaciones.

Con esto en mente y considerando otros estudios internacionales como el realizado por PwC, IBM, EY, CISCO, Verizon, ESET, se procederá a analizar los resultados de la Encuesta Nacional de Seguridad Informática ACIS 2018.

Estructura de la encuesta

El estudio contempla 43 preguntas repartidas en varias secciones sobre diferentes asuntos.

Demografía: Describe la información del encuestado, cuáles son las tareas que realiza, la visión de la seguridad, además de los roles que en tal sentido

puedan existir dentro de su organización. Datos que permiten ubicar el sector al que pertenece, el tamaño y tipo de empresa.

Presupuestos: Relaciona todos los aspectos asociados con los recursos financieros destinados en materia de seguridad y, sobre todo, en qué se concentra la inversión de dichos recursos.

Incidentes de seguridad: Muestra los detalles y tipos de incidentes presentados, un barrido por las prácticas más importantes en el manejo y diligencia de la evidencia digital, como herramienta en la persecución de los ciberdelincuentes.

Herramientas y prácticas de seguridad: Se refiere a las prácticas comunes en materia de seguridad, ese conjunto de acciones que permiten a las organizaciones definir una postura clara en materia de protección.

Políticas de seguridad: Busca conocer el estado de las políticas de seguridad, la práctica de la gestión de riesgos y su integración en el contexto organizacional.

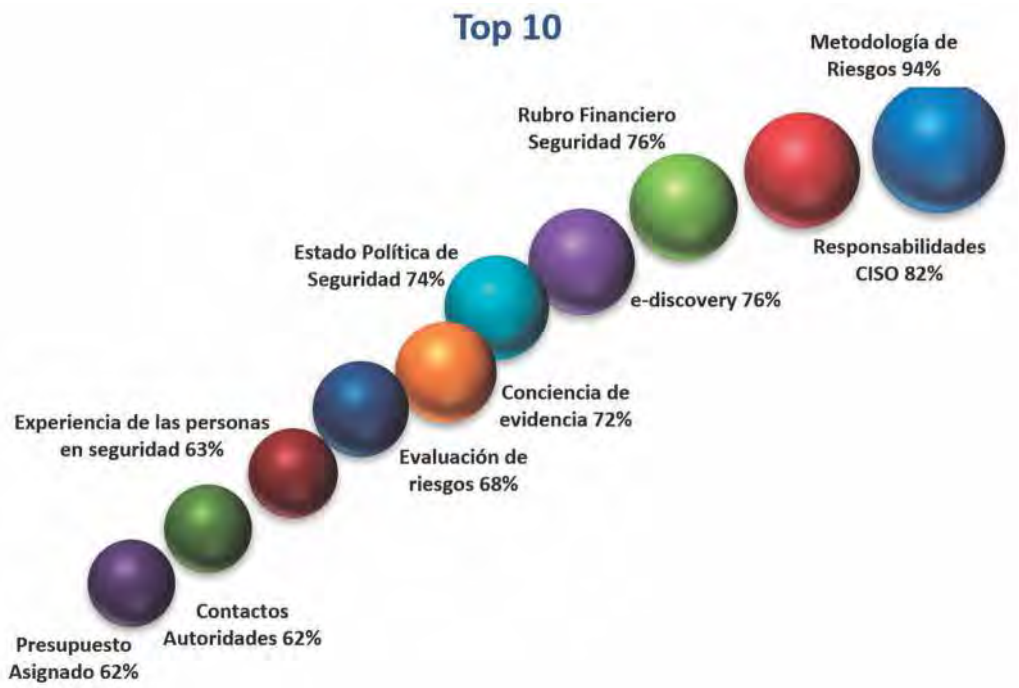
Capital intelectual: Busca definir cómo son las áreas de seguridad y las características básicas en materia de experiencia, formación y capacitación de los profesionales de seguridad. Muestra también la relación de las instituciones de educación superior frente a una realidad tan cambiante.

Temas emergentes: En esta sección se analizan varios aspectos, entre ellos: la percepción del futuro en materia de ciberseguridad; la vinculación de los directivos de la organización en la ciberseguridad empresarial, además de la responsabilidad y el papel del líder de seguridad en el desarrollo de la dinámica de protección de la empresa.

Hallazgos principales

De la información recogida en este estudio se muestran en la siguiente gráfica los aspectos clasificados como importantes por todos los encuestados y reunidos en un grupo denominado top 10.

En la gráfica 1 se encuentran los datos más relevantes de la encuesta. El 94% de los encuestados reconoce usar una metodología de gestión de riesgos como herramienta para admi-nistrar los riesgos en materia de segu-ridad digital. Con base en los resulta-dos, un 82% considera que la respon-sabilidad del profesional de seguridad en las organizaciones está centrada en velar por la protección de la información empresarial. Un 76% indica que existe un rubro definido para la seguridad de la información, mientras que un 76% no tienen estrategias de ediscovery, como instrumento para la administración de la evidencia digital ni soporte de las pruebas ante litigios judiciales. Tales porcentajes muestran que no es una práctica aún bien entendida. Un 74% reconoce la importancia de la evidencia digital y tiene conciencia de los procesos relacionados con la identificación, preservación y análisis de la evidencia digital. La evolución de la seguridad dentro de las empresas colombianas aumenta y se ve reflejada en que el 74% de los participantes manifestaron poseer un modelo de políticas de seguridad aprobado y conocido por todos los miembros de la organización. Aunque existe una conciencia clara para usar la gestión de



Gráfica 1: Top 10 de Resultados

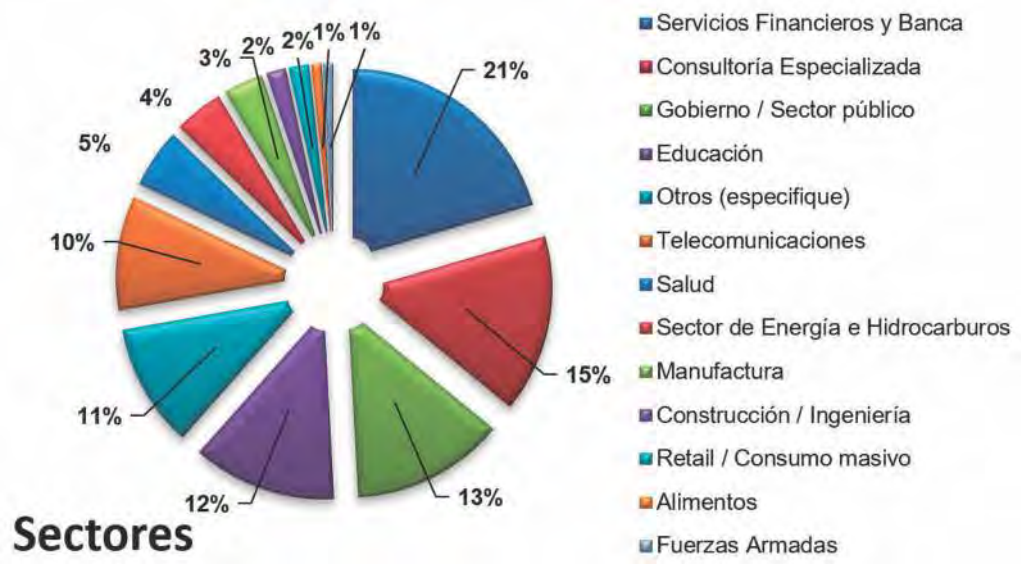
riesgos, sólo el 68% identifica en sus modelos los riesgos relacionados con la seguridad digital, lo que significa la existencia de retos interesantes en el uso de la gestión de riesgos como instrumento para la toma de decisiones en torno a la seguridad digital. La experiencia de los profesionales de seguridad es otro de los datos relevantes de esta encuesta, el 63% de los participantes manifiesta que el profesional de seguridad debe contar, por lo menos, con dos años de experiencia para ocupar la posición en las distintas organizaciones de Colombia. Por otra parte, la cooperación se ha convertido en un factor fundamental en nuestro país; de ahí que el 62% de los encuestados manifiesta mantener contacto con las autoridades nacionales e internacionales, frente a los incidentes de seguridad o ciberseguridad. El último dato relevante del top 10 está centrado en los presupuestos de seguridad; un 62% de los participantes desconoce el monto asignado para el año 2018.

Demografía

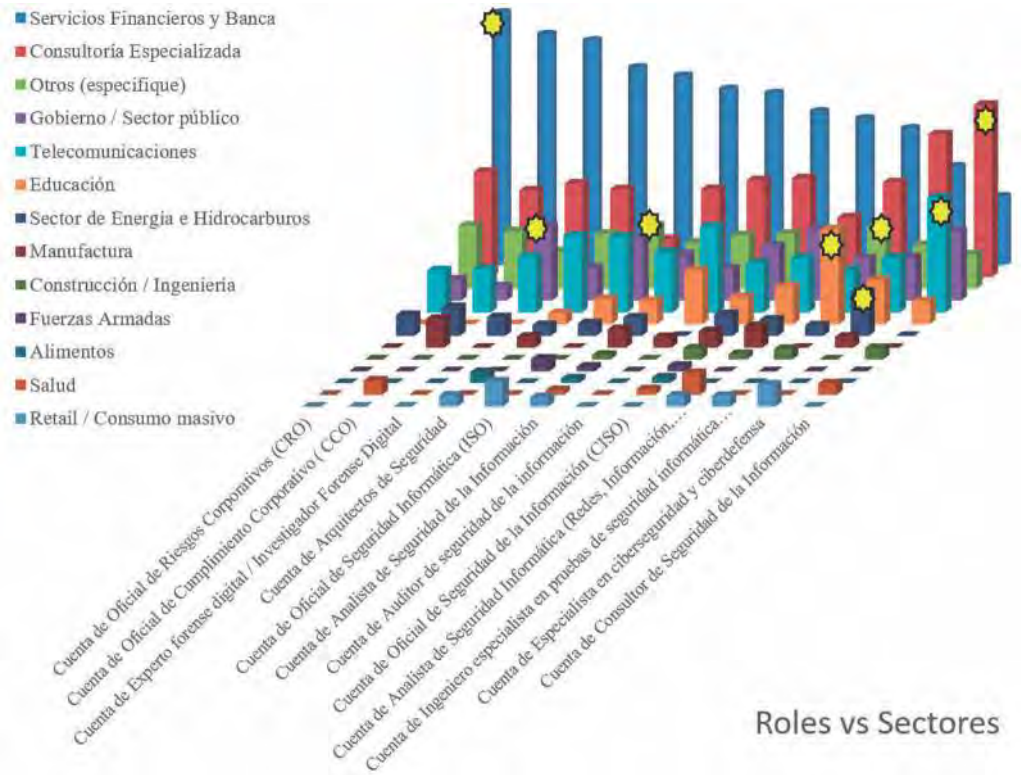
Sectores participantes

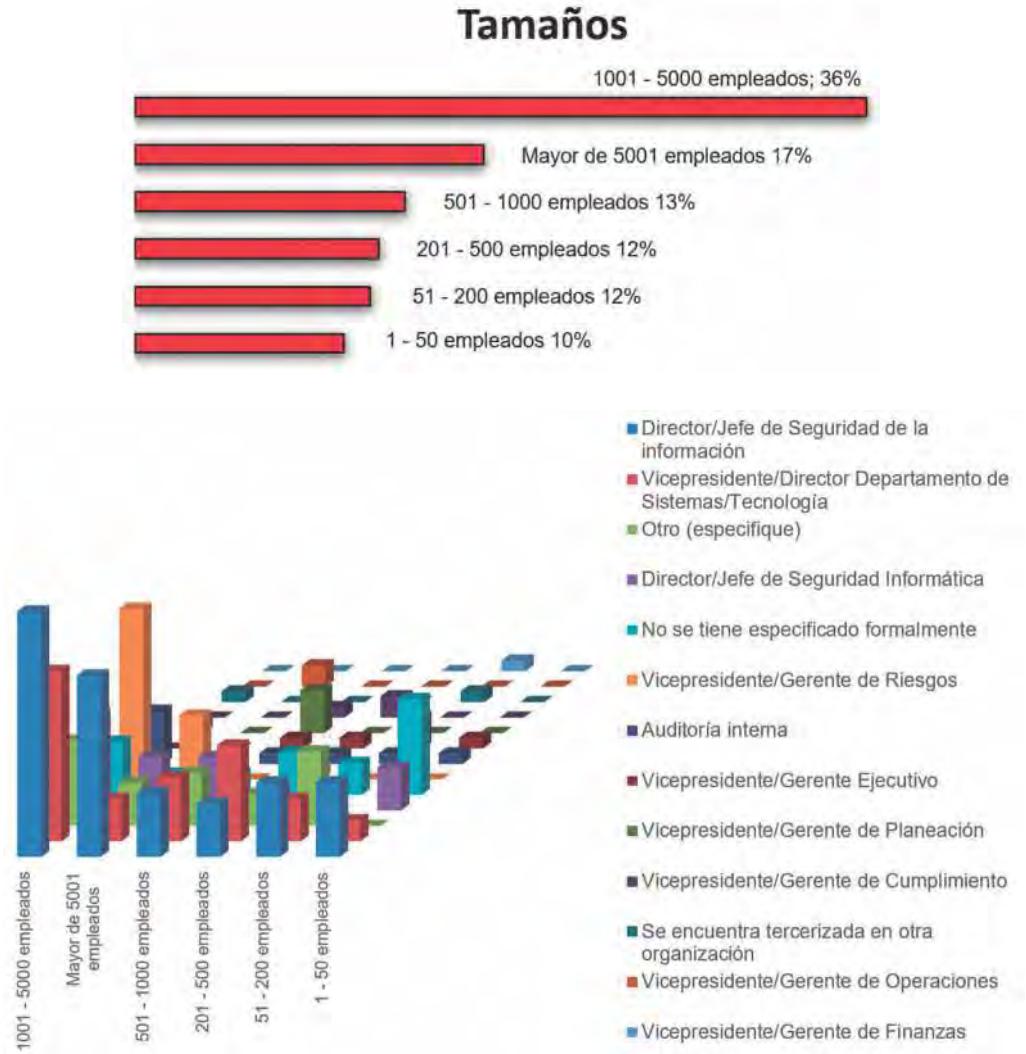
La gráfica 2 refleja la participación de 13 sectores de la economía colombiana. Los tres segmentos con mayor injerencia están compuestos por el sector financiero, servicios de consultoría especializada y el Gobierno.

La Gráfica 3 muestra el tamaño de las empresas en Colombia, de acuerdo con el número de empleados. Como se puede observar, el 53% de la mues-



Gráfica 2: Sectores participantes





Gráfica 3: Tamaño de las empresas. Dependencia vs. tamaño

tra incluye a empresas de gran tamaño más de 1000 en Colombia.

La Gráfica 4 muestra los cargos de los encuestados, entre los que se cuentan auditores, profesionales de TI, profesionales de seguridad, CISOs. Así mismo, figuran otras clasificaciones para los profesionales de seguridad digital en el país, tales como analistas y profesionales de planta de seguridad, entre otros.

En la Gráfica 5 se observan las tareas realizadas por los profesionales de seguridad dentro de las organizaciones. El porcentaje más alto está representado en velar por la protección de la información empresarial, definir los controles de TI en materia de seguri-

Gráfica 4: Cargos de los encuestados

dad digital y establecer un modelo de políticas en materia de seguridad digital.

La Gráfica 6 muestra de quién depende el área de seguridad. Los datos indican que el área de seguridad depende de una dirección propia. Por otro lado, están las áreas de tecnología con la responsabilidad de dirigir la seguridad digital en las empresas.

En la Gráfica 7 se observan los roles dentro de una organización, en materia de seguridad digital. En Colombia figuran los analistas de seguridad (in-

Gráfica 5: Funciones del responsable de seguridad

Gráfica 6: Dependencia del área de Seguridad

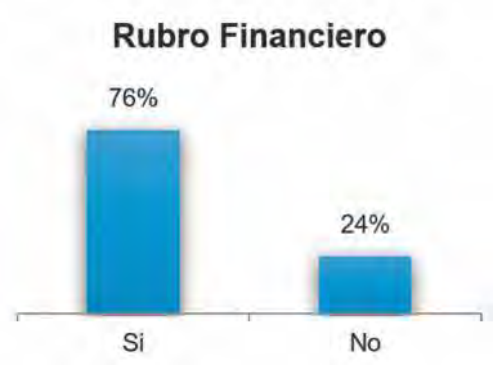
formación e informática); le sigue el cargo denominado CISO, al que se suman los ingenieros de pruebas, entre los principales roles

Presupuestos

La realidad colombiana es muy interesante, en materia de presupuestos en

Gráfica 7: Roles de Seguridad

el mundo de la seguridad digital. El 76% de los participantes manifiesta que sí tiene presupuesto asignado a la seguridad digital de sus organizaciones, lo cual se refleja en la Gráfica 8.



Gráfica 8: Presupuesto de Seguridad

La Gráfica 9 muestra el monto del presupuesto en relación con el presupuesto global; el 46% de los encuestados lo conoce, mientras que el 54% dice no conocer o no tener la información. La Gráfica 10 refleja la distribución de los presupuestos en dólares. El 39% de los participantes tiene conocimiento de los valores asignados para el 2018, mientras el 62% manifiesta no conocer los valores asignados. Esto se puede explicar, toda vez que los cargos de mayor participación están compuestos por auditores y los profesionales de las áreas de tecnologías que pueden no conocer los detalles internos de las áreas de seguridad. La otra gran razón para que se de esta realidad es que muchos de los roles de

Gráfica 9: Porcentaje del presupuesto Global

Gráfica 10: Presupuesto de Seguridad

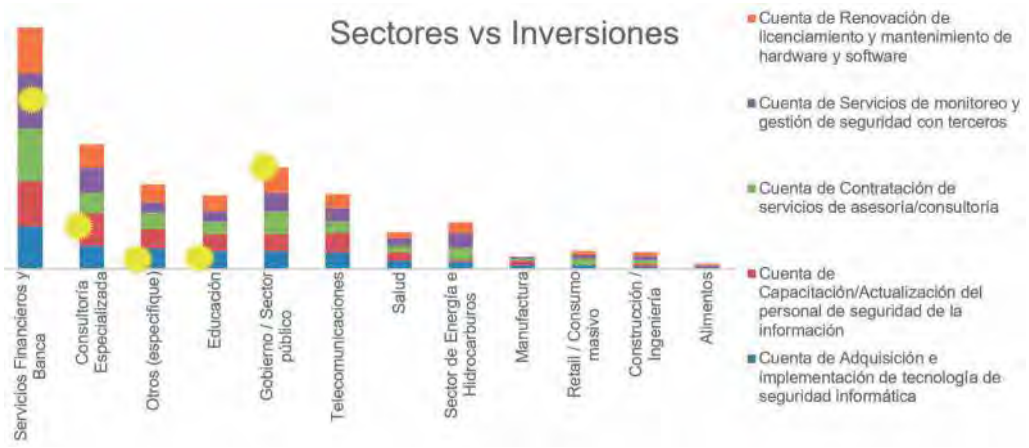
Gráfica 11: Inversión de Seguridad

las organizaciones están asociados con los analistas de seguridad, quienes pueden no conocer estos detalles. La Gráfica 11 muestra cómo se están realizando las inversiones en materia de seguridad. La inversión en tecnologías de seguridad es la parte más importante, seguida de la renovación del licenciamiento de algunas tecnologías en materia de seguridad digital; los servicios de consultoría y asesoría ocupan el tercer lugar; la tercerización de servicios, en materia de seguridad, están en cuarto lugar, y la capacitación y actualización de los profesionales de seguridad es el último criterio sobre los presupuestos. La Gráfica 12 muestra en dólares, los montos de la inversión en diferentes tópicos. La franja de recursos financieros menos usada corresponde al rango entre $US70.000 a $US90.000 dólares.

Incidentes

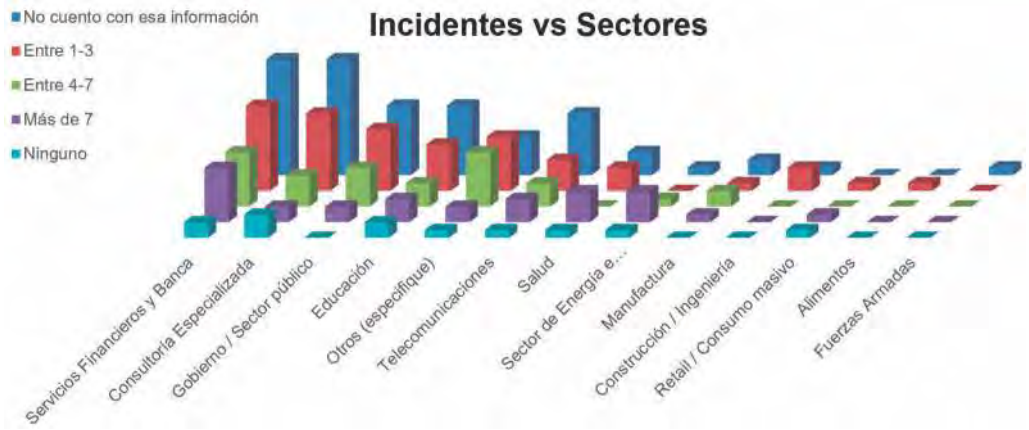
En Colombia se mantiene la tendencia en materia de incidentes de seguridad en concordancia con las tendencias internacionales. Tales desafíos, en términos de preparación y atención, son una exigencia para las organizaciones.

La Gráfica 13 muestra la cantidad de incidentes que se presentan en Colombia, según los participantes. El

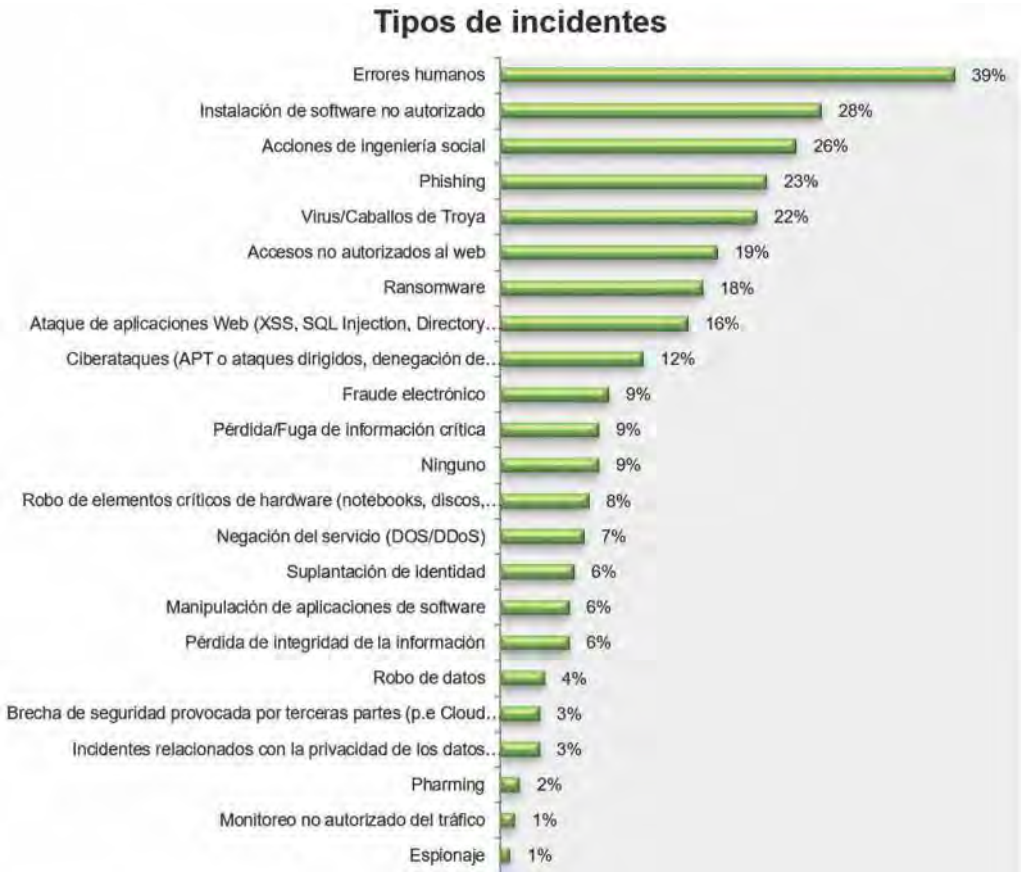


Gráfica 12: Montos en dólares de las inversiones de seguridad. Sectores vs. inversiones

65% de ellos manifiesta haber tenido, por lo menos, un incidente de seguridad o ciberseguridad en sus organizaciones. El 35% de los participantes no tiene información al respecto.



Gráfica 13: Cantidad de Incidentes. Incidentes vs sectores



Gráfica 14: Tipos de Incidentes de Seguridad

La Gráfica 14 relaciona los tipos de incidentes que se presentaron en las organizaciones. En ella se relacionan los errores humanos, la instalación de *software* malicioso y la ingeniería social como los de mayor incidencia.

La Gráfica 15 muestra la acción de los encuestados frente a un incidente, en términos de las notificaciones respectivas. Los datos reflejan que, ante un incidente y su identificación, el 52% de los participantes lo notifican a la propia organización, y el 31% al equipo de respuesta a incidentes. La Gráfica 16 refleja la forma como mejor se comunican los incidentes, máxime cuando éstos deben ser notificados a entes externos a la organización. El 62% de los encuestados manifiesta que con canales seguros se debe realizar este tipo de procedimientos.

En la Tabla 1 se relacionan los ítems asociados a la evidencia digital, como parte fundamental del proceso de gestión de incidentes. El 72% de los encuestados tiene conciencia para identificar, preservar, y analizar la evidencia como parte de dicho proceso. No obstante, sólo el 22% realiza procedimientos formales y un 30% no formales. En esa misma medida, el 70% dice no tener procedimientos de e-discovery o descubrimiento electrónico, como herramienta para soportar los posi-

Gráfica 15: Notificaciones de un Incidente

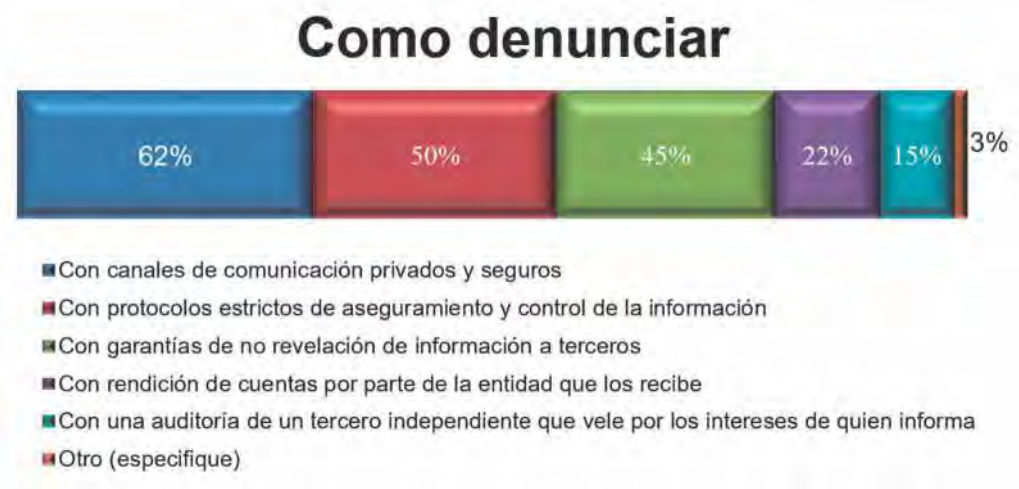
bles litigios o reclamaciones legales. Es importante señalar que, cerca del 62% de los participantes, tiene contacto con autoridades de orden nacional e internacional, como parte de las prácticas claves en los procesos de gestión de incidentes.

Herramientas

La Gráfica 17 muestra el uso de las evaluaciones de seguridad como una de las prácticas más usadas. Un 82% de los participantes manifiesta hacer uso de esta práctica como instrumento clave para validar el estado de la seguridad digital de la organización. El 39% de los participantes usa esta práctica una vez al mes; el 34% entre dos y 4 veces al año; el 18% dice no usarla y el 9% usa más de 4 veces al año los procesos de evaluaciones de seguridad en sus organizaciones.

Conciencia de la evidencia digital	**72%**
Procedimientos de evidencia digital	53%
Estrategia de E-Discovery	24%
Contacto con autoridades	62%

Tabla 1: Evidencia Digital



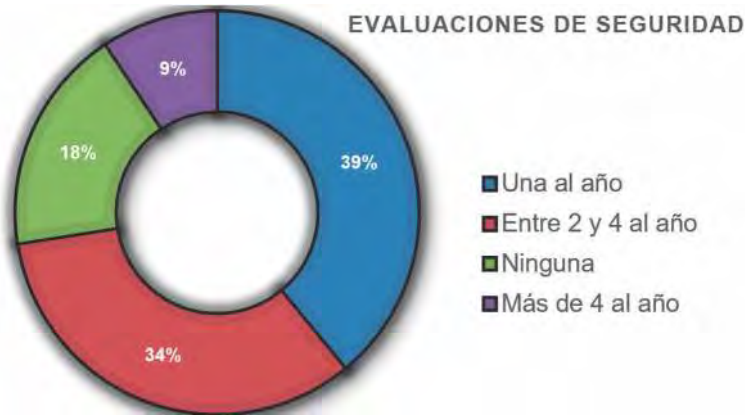
Gráfica 16: Mecanismos para denunciar

La Gráfica 18 indica cuáles son los mecanismos de seguridad comúnmente usados en las organizaciones. La Virtual Private Network (VPN), los *Firewalls*, y las soluciones *Antimalware* son los mecanismos más usados en las organizaciones colombianas.

Como parte de las prácticas en materia de seguridad los participantes se mantienen notificados de las fallas de seguridad, a través de múltiples mecanismos, entre los que se destacan la lectura de artículos y revistas especializadas (48%); la cooperación con colegas (47%); la notificación de los proveedores (42%); alertas de Computer Security Incident Respond Team (CSIRT), (35%) y la lectura de listas de seguridad (31%). Cabe señalar que sólo un 8% no usa este tipo de prácticas, a la hora de estar informado sobre las fallas de seguridad.

Políticas

La Gráfica 19 refleja el estado de las políticas de seguridad en las organizaciones colombianas; el 90% de los participantes manifiesta tener una o algu-

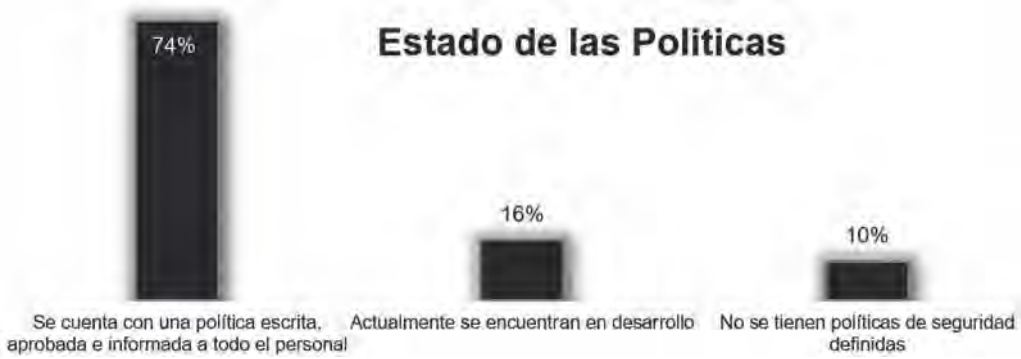


Gráfica 17: Evaluaciones de Seguridad

Gráfica 18: Mecanismos de Seguridad

nas en sus diferentes estadios. En comparación con años anteriores, se observa un claro crecimiento notorio.

Las organizaciones y sus responsables de seguridad entienden que las políticas no son el único ni el ultimo instrumento para construir posturas de seguridad. Al indagar sobre los obstáculos por los cuales no hay posturas adecuadas en materia de seguridad en las empresas, un 49% de los partici-



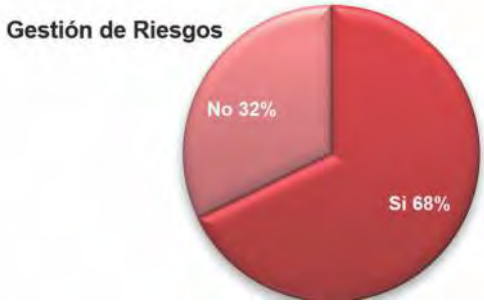
Gráfica: 19 Estado de las Políticas

Gráfica 20: Obstáculos de la Seguridad

pantes señala como factor más importante, la ausencia de una cultura de seguridad, como lo muestra la Gráfica 20.

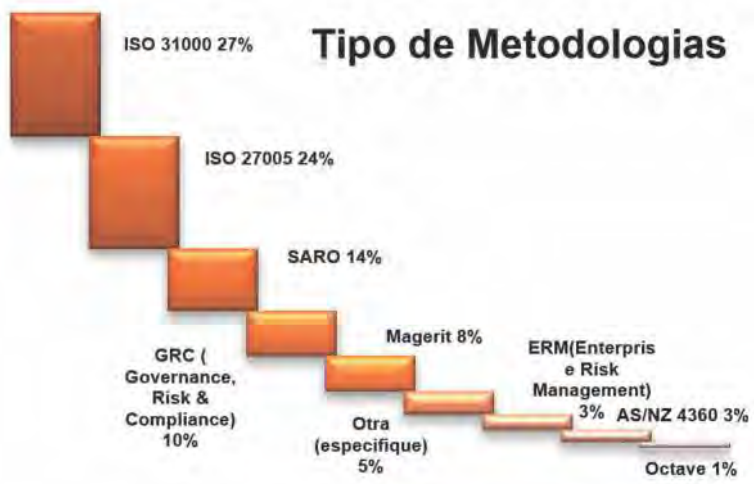
La gestión de riesgos como parte estructural de las funciones y tareas de los responsables de seguridad y sus organizaciones es otro de los componentes claves. En la Gráfica 21, el 68% de los participantes hace una evaluación de riesgos de seguridad digital y la incluyen en sus ejercicios globales de gestión de riesgos. En la Gráfica 22, el 97% realiza el ejercicio en un rango entre una y más de dos veces en el año, lo que ratifica la importancia de realizar estos ejercicios como herramientas para la toma de decisiones en las organizaciones. El Foro Económico Mundial en su informe del año 2018, señala los riesgos cibernéticos como una de las amenazas más probables de este tiempo, de ahí la importancia en el uso de estas prácticas y como herramientas para la construcción de posturas digitales consistentes y coherentes en la realidad colombiana.

Al indagar por qué no se realiza la gestión de riesgos de seguridad, se encuentra que el 38% lo hace dentro del proceso corporativo de gestión de riesgos. Este dato es muy interesante porque indica que la seguridad digital es transversal a los procesos, las perso-



Gráfica 21: Gestión de Riesgos de Seguridad

Gráfica 22: Cantidad de Gestión de Riesgos en Seguridad



Gráfica 23: Tipos de Metodología

nas, además de proporcionar una visión integral para el negocio. La Gráfica 23 muestra el tipo de metodologías usadas al realizar los ejercicios de gestión de riesgos de seguridad; la ISO 31000, con un 27%, es la metodología más usada. La Gráfica 24 representa el tipo de riesgos asociados a los

Gráfica 24: Tipos de Riesgos

Gráfica 25: Marcos de trabajo usados

incidentes de seguridad. La categoría de riesgos operativos es la más usada para esta situación.

La Gráfica 25 ilustra el uso de los distintos marcos de trabajo (*frameworks*) usados en las organizaciones colombianas: ISO/IEC 2700, ITIL y Cobit 5 son los más usados. La Gráfica 26 refleja las regulaciones a las que las organizaciones están sometidas; en el caso colombiano, el 63% de los participantes manifiesta que sí existen regulaciones a las que sus organizaciones se ven sometidas. La tendencia internacional se orienta a que, cada vez más, existirán regulaciones más globales. La regulación GDPR (General Data Protection Regulation) nace como una necesidad de la Comunidad Europea (EU), de gran impacto a nivel global.

Gráfica 26: Regulaciones o normativas

Capital intelectual

Las áreas de seguridad de la información en Colombia están formadas por grupos de una a cinco personas, de acuerdo con los participantes. La Gráfica 27 muestra el grupo de organizaciones que cuentan con un recurso dedicado a la seguridad (81%). La Gráfica 28 resalta que el tiempo de experiencia promedio para que los profesionales de seguridad sean contratados en Colombia es superior a dos (2) años y su experiencia es importante (91%) y necesaria para desempeñar un cargo en materia de seguridad. La Gráfica 29 indica que la certificación que poseen en la actualidad los profesionales de seguridad, corresponde a la de Auditor ISO/IEC 27001. Por otro lado, también se observa que estos profesionales buscan en el futuro cercano certificaciones como la Certified Information Security Mana-

Gráfica 27: Recursos dedicados a la Seguridad

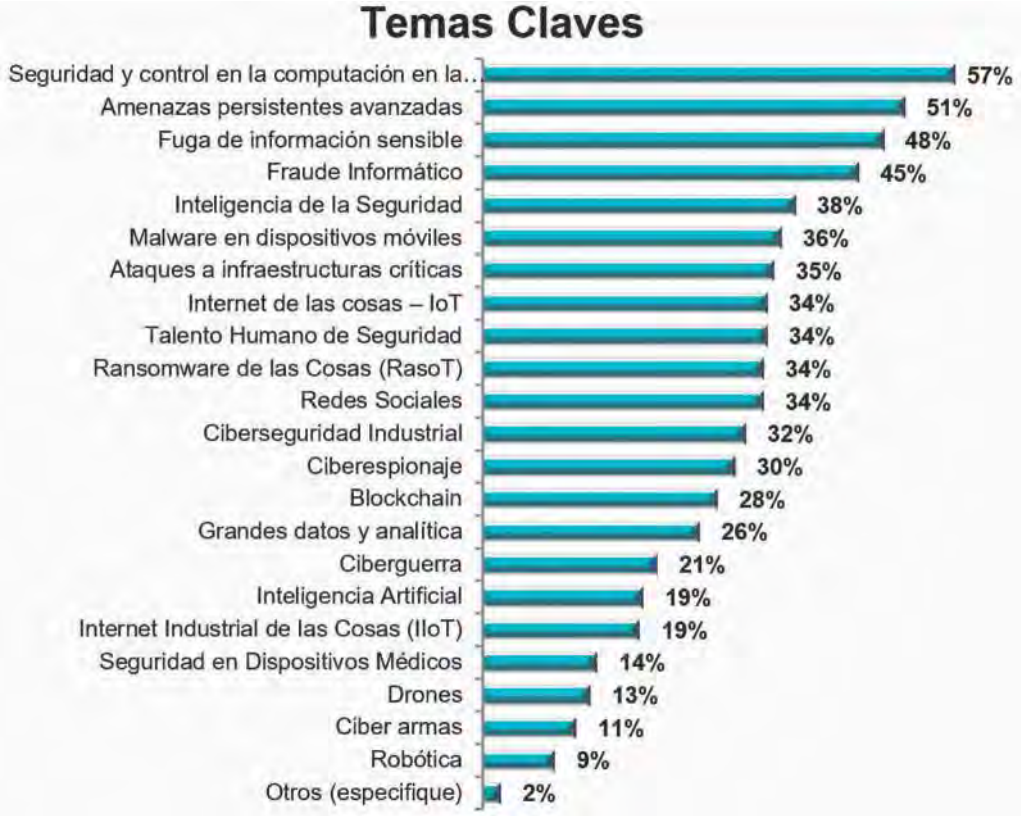
Gráfica 28: Experiencia del profesional

Gráfica 29: Certificaciones poseídas vs deseadas

Gráfica 30: Papel de la educación

ger (CISM), como oportunidades para mejorar sus perfiles. La tendencia internacional lo ratifica, en el sentido de que los perfiles de los profesionales de seguridad se pueden mejorar con las ofertas de certificaciones y educación formal.

La Gráfica 30 indaga sobre la forma en que la educación ha participado en la



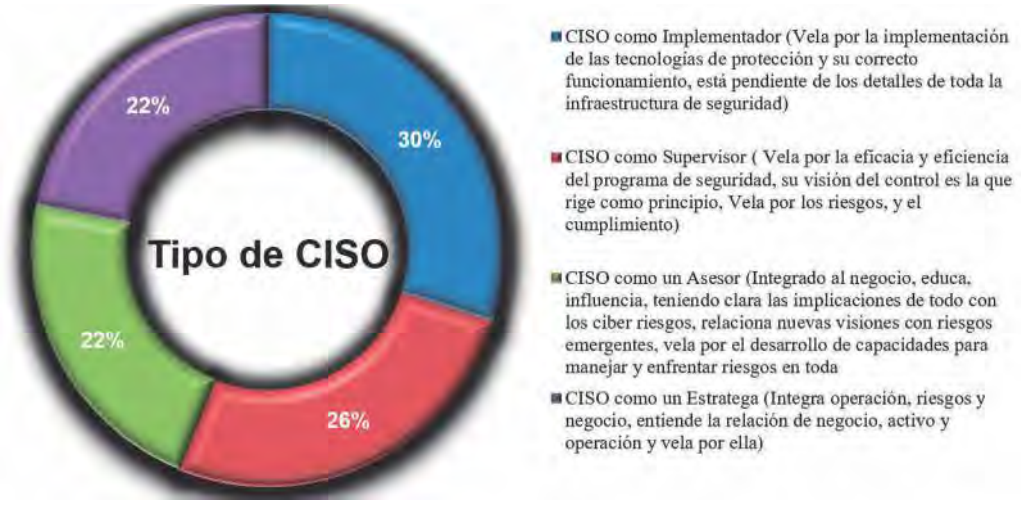
Gráfica 31: Desafíos del 2018

Gráfica 32: Involucramiento de los Directivos

formación de los profesionales de seguridad. En este sentido, el punto a resaltar por parte de los participantes es que no existe la suficiente investigación, que es escasa o insuficiente en materia de seguridad digital, con un 41%. De igual forma se advierte una ligera mejora en la formación académica de los profesores, en temas de seguridad y control respecto del año anterior.

Temas emergentes

La Gráfica 31 muestra los temas inherentes a los profesionales de seguridad durante el año 2018, los cuales pueden producir importantes desafíos



Gráfica 33: Cómo ven al CISO

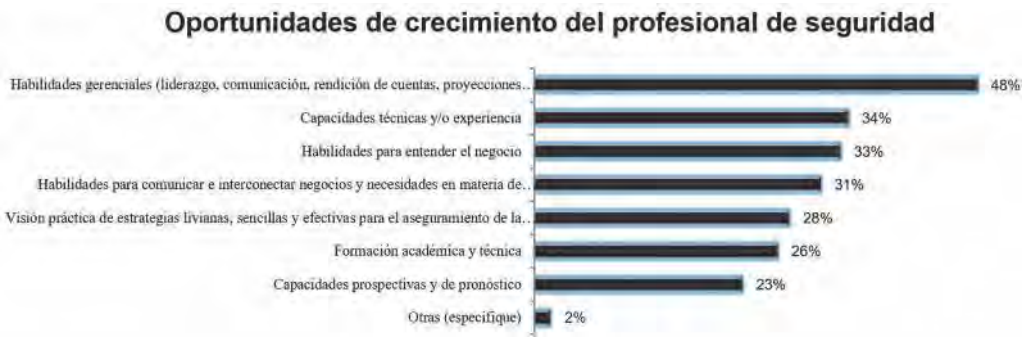
en el desarrollo de los distintos negocios. El más relevante, la computación en la nube como uno de los grandes desafíos de las organizaciones colombianas. Las amenazas avanzadas continúan en la lista, de la misma manera que la fuga de información sensible, como temas claves para tener presentes.

Una de las grandes preocupaciones de muchos profesionales de seguridad está centrada en sus juntas directivas y cómo se deben vincular a todas las iniciativas en materia de ciberseguridad; así mismo lo manifiestan los distintos referentes internacionales. En este sentido, la Gráfica 32, muestra según los participantes el nivel de involucramiento de los directivos de las organizaciones en Colombia. En este sentido, se ratifica la tendencia internacional orientada a que cada vez más los niveles ejecutivos (C-Levels) y los niveles directivos (Board Level) están involucrados en la realidad de la ciberseguridad y la seguridad digital de sus empresas. En el contexto colombiano, el 71% de los encuestados manifiesta que de alguna manera están estos niveles involucrados; sólo el 29% de los participantes no ve que estos cuerpos directivos se involucren.

Líder de Seguridad de la Información

Las Gráficas 33, 34 y 35 reflejan la forma como el CISO se ve, se desenvuelve y cómo puede evolucionar en el contexto de las organizaciones nacionales. La Gráfica 33 muestra la forma como es visto el profesional de seguridad. Vale anotar que continúa la visión del CISO como un implementador de las tecnologías de protección; así lo ratifican los datos obtenidos, considerando que las inversiones de seguridad precisamente se centran en ello; y, en torno a los top en términos de controles usados, las herramientas tecnológicas están en los primeros lugares. Una segunda mirada al profesional de seguridad está relacionada con el *compliance*; en otras palabras, un profesional que vela por el cumplimiento regulatorio, el control y su implementación, un asesor que se encarga de educar, influenciar en alguna medida a toda la organización; y, por último, un profesional estratega o líder que se integra dentro de la empresa y ve el

Gráfica 34: Entrega de información del profesional de seguridad



Gráfica 35: Camino de crecimiento de un profesional de seguridad

mundo de una manera distinta, en términos de la seguridad.

La Gráfica 34 muestra la forma como el líder de seguridad se comunica con la organización, en todos sus niveles. La comunicación es una de las nuevas herramientas claves que deben ser usadas por los profesionales de seguridad, como lo manifiestan algunos estudios internacionales. En primer lugar, en Colombia ellos suministran información técnica, seguida por la información relacionada con los riesgos de seguridad de la información y luego sobre la gestión y las brechas e incidentes de seguridad. En la totalidad de los datos se puede ver que, efectivamente, el profesional de seguridad entrega algún tipo de información.

La Gráfica 35 muestra las oportunidades de crecimiento y mejora en las que los profesionales de seguridad pueden trabajar, como parte del cierre de brechas existentes. En primer lugar, las habilidades gerenciales son uno de los elementos identificados como aspecto a mejorar; las capacidades técnicas y la experiencia figuran en el siguiente nivel, seguidas por la necesidad de involucrar el entendimiento del negocio como parte de las capacidades de los profesionales de seguridad.

Reflexiones finales

Año tras año, el estudio muestra un afianzamiento de la seguridad digital como un instrumento corporativo en las empresas colombianas. En este contexto, cada vez más incierto, son necesarios los pensamientos amplios que involucren a los actores y los lleven a pensar en un replanteamiento de la protección de la información, sin perder de vista lo ya alcanzado, para enfrentar la realidad del mundo en que se desenvuelven.

Cada vez más, las organizaciones se enfrentan a una realidad digitalmente modificada, en la que las nuevas tecnologías permean cada uno de los ambientes organizacionales y personales. Esta creciente expansión digital hace de la realidad un mejor lugar; se enfrentan nuevos y desafiantes riesgos, que invitan a la reflexión en procura de proteger el valioso activo de la información, encaminada a lograr posiciones más confiables en un mercado competitivo y exigente.

Por lo tanto, los ejecutivos de seguridad de esta nueva era se enfrentan de una manera más directa a otros escenarios dinámicos que demandan reacciones rápidas; pero, sobre todo, se

trata de espacios que exigen anticiparse a observar los entornos cambiantes y superpuestos, en procura de la protección de la información.

En la realidad colombiana, los datos muestran que los esfuerzos se vienen haciendo, que año a año las demandas de la realidad digitalmente modificada transforman la visión de la seguridad. El contexto internacional indica la misma tendencia.

En la realidad nacional se pueden concluir los siguientes aspectos:

1. De acuerdo con los resultados obtenidos, el sector financiero, la consultoría especializada y el Gobierno, les interesa participar y conocer la realidad de la seguridad, tendencia observada en diferentes informes publicados sobre seguridad y ciberseguridad.

2. En las organizaciones colombianas, las áreas de seguridad y ciberseguridad tienen dos posiciones marcadas. Algunas cuentan con una dirección propia y definida, mientras otras dependen formalmente de las áreas de tecnología. Las compañías de gran tamaño, con más de 1000 empleados, son las que tienen mayor claridad en torno a un área independiente y a un director de seguridad. En tales empresas grandes, el área de seguridad depende de las direcciones como la de gestión de riesgos. Es interesante observar entre las organizaciones de todos los tamaños, el bajo porcentaje que no tiene un cargo o responsabilidades definidas.

3. La posición del profesional de seguridad continúa su proceso de afianzamiento dentro de las organizaciones, en una realidad digitalmente modificada. De asesor técnico, se espera que el CISO se convierta en asesor, suministrando información estratégica para la toma de decisiones, de tal manera que las vías de comunicación con los miembros de la empresa sean más expeditas, en busca de proteger la información.

4. A nivel nacional, se mantiene la sólida tendencia de usar mecanismos tecnológicos como las principales herramientas de protección. De igual manera, se abre camino la seguridad más allá de unas implementaciones tecnológicas y en la protección, una oportunidad para construir nuevos estándares alrededor de la cultura organizacional.

5. El poder de las anomalías digitales, de los adversarios y de la realidad digital se entiende cada vez más en el marco de las organizaciones colombianas. Más allá de lo técnico, se registran los errores humanos y, en tal sentido, es necesario pasar de procesos de sensibilización al cambio de comportamientos, liderado por los responsables de la seguridad, con el ánimo de crear una nueva cultura alrededor de entornos digitalmente modificados. Así mismo, es necesario gestionar unos programas de seguridad que permeen todos los niveles organizacionales, sobre prácticas centradas en los diferentes grupos de interés, dirigidas a construir posturas de seguridad diferentes, basadas en los desafíos que debe asumir el talento humano.

6. Las nuevas tecnologías como Cloud, IoT, IA, Machine Learning entre otras, están cambiando la concepción del mundo, la forma de interactuar y los retos a los que se enfrentan las organizaciones a nivel nacional e inter-

nacional. De ahí que los profesionales de seguridad deban tener claridad para profundizar en estas nuevas tendencias y su uso. En ambientes internacionales es limitado el uso de la nube, producto del desconocimiento y los riesgos que ésta implica.

7. Los resultados de la encuesta reflejan que, a la hora de implementar modelos de seguridad, las organizaciones usan algún estándar, hecho motivado más por las regulaciones que por una intención de proteger, lo que genera el debate nacional e internacional alrededor de tales asuntos. La meta de la protección organizacional no debe estar sujeta al cumplimiento.

En resumen, el panorama general de la seguridad en Colombia muestra cambios importantes y se mueve en la misma línea de las tendencias internacionales en los aspectos revisados. Se registran nuevos desafíos y una gran oportunidad para potenciar a las organizaciones, en procura de construir posturas de seguridad digital más confiables y resilientes, encaminadas a mejorar e impulsar su competitividad actual y futura.

Referencias

Clinton Larry. (2017) Cyber-Risk Oversight. Director´s Handbook Series. NACD (National Association of Corporate Directors). Recuperado de: https://www.nacdonline.org/files/FileDownloads/NACD%20Cyber-Risk%20Oversight%20Handbook%202017.pdf

Choudhary, U. (2015) This Might Be The Next Coveted Leadership Position Of 2015. *F@stcompany Magazine.* Recuperado de: https://www.fastcompany.com/3043376/how-to-earn-respect-from-the-hottest-seat-in-leadership-today

World Economic Forum. (2018). The Global Risks Report 2018 13th Edition. Mayo. Recuperado de: http://www3.weforum.org/docs/WEF_GRR18_Report.pdf

World Economic Forum. (2018). Cyber Resilience Playbook for Public-Private Collaboration. Mayo. Recuperado de: http://www3.weforum.org/docs/WEF_Cyber_Resilience_Playbook.pdf

ISACA. (2018). State of Cybersecurity 2018. Recuperado de: https://cybersecurity.isaca.org/state-of-cybersecurity

Deloitte. (2017). Cybersecurity and the role of internal audit An urgent call to action. Recuperado de: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-risk-cyber-ia-urgent-call-to-action.pdf

Deloitte. (2017). The value of visibility Cybersecurity risk management examination. Recuperado de: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-the-value-of-visibility-cybersecurity-risk-management-examination.pdf

Deloitte. (2017). Assessing cyber risk Critical questions for the board and the C-suite. Recuperado de: https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-ers-assessing-cyber-risk.pdf

IBM. (2018). IBM X-Force Threat Intelligence Index 2018. Recuperado de: https://microstrat.com/sites/default/files/security-ibm-security-solutions-wg-

research-report-77014377usen-20180329.pdf

Raj Samani, McAfee Chief Scientist. (2018) Navigating a Cloudy Sky. Recuperado de: http://www.redseguridad.com/content/download/73021/580227/file/rp-navigating-cloudy-sky.pdf

CISCO. (2018). Reporte Anual de Seguridad 2018. Recuperado de: https://www.cisco.com/c/es_co/products/security/security-reports.html

PwC. (2017). Revitalizing privacy and trust in a data-driven world. Recuperado de: https://iapp.org/media/pdf/resource_center/revitalizing-privacy-trust-in-data-driven-world.pdf

PwC. (2018). The Anxious Optimist in the Corner Office. Recuperado de: https://www.pwc.com/gx/en/ceo-survey/2018/pwc-ceo-survey-report-2018.pdf

PwC. (2017). Strengthening digital society against cyber shocks. Recuperado de: https://www.pwc.com/us/en/services/consulting/cybersecurity/library/information-security-survey/strengthening-digital-society-against-cyber-shocks. html

PwC. (2017). Moving forward with cybersecurity and privacy. Recuperado de: https://www.pwc.com/kr/ko/industries/automotive/201512_moving-forward-with-cybersecurity-and-privacy_en. pdf

PwC. (2017). Toward new possibilities in threat management. Recuperado de: https://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/assets/gsiss-report-cybersecurity-privacy-possibilities.pdf

Verizon. (2018). 2018 Data Breach Investigations Report. Recuperado de: https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_execsummary_en_xg.pdf

Ponemon Institute. (2018). 2018 Cost of Insider Threats: Global. Recuperado de: https://www.observeit.com/ponemon-report-cost-of-insider-threats/

Ponemon Institute & IBM. (2018). The Third Annual Study on the Cyber Resilient Organization. Recuperado de: https://info.resilientsystems.com/hubfs/IBM_Resilient_Branded_Content/White_Papers/2018_Cyber_Resilient_Organization_Study.pdf

Ponemon Institute & F5 Networks. (2017). The Evolving Role of CISOs. Recuperado de: https://f5.com/Portals/1/PDF/labs/Evolving_Role_of_CISOs_Aug2017.pdf?ver=2017-09-18-100218-007

EY. (2017). Cyber resiliency: evidencing a well-thought-out strategy. Mayo. Recuperado de: http://www.ey.com/Publication/vwLUAssets/EY-cyber-resiliency-evidencing-a-well-thought-out-strategy/$FILE/EY-cyber-resiliency-evidencing-a-well-thought-out-strategy.pdf

EY. (2017). An integrated vision to manage cyber risk. Recuperado de: http://www.ey.com/Publication/vwLUAssets/ey-an-integrated-vision-to-manage-cyber-risk/$File/ey-an-integrated-vision-to-manage-cyber-risk.pdf

EY. (2017). Cybersecurity regained: preparing to face cyber attacks. Recu-

perado de: http://www.ey.com/Publication/vwLUAssets/ey-cybersecurity-regained-preparing-to-face-cyber-attacks/$FILE/ey-cybersecurity-regained-preparing-to-face-cyber-attacks.pdf

Accenture. (2018). Gaining Ground On The Cyber Attacker. Recuperado de: https://www.accenture.com/t20180416T134038Z__w__/us-en/_acnmedia/PDF-76/Accenture-2018-state-of-cyber-resilience.pdf

Gemalto. (2018). 2017 The Year of Internal Threats and Accidental Data Breaches. Recuperado de: https://breachlevelindex.com/assets/Breach-Level-Index-Report-2017-Gemalto.pdf

Rachel Linthwaite, Market Impact Consultant. (2017) Drop A Pin At The Intersection Of Digital Experience And Security. Forrester Consulting. Mayo. Recuperado de: https://www.akamai.com/us/en/multimedia/documents/white-paper/forrester-digital-maturity-thought-leadership-white-paper.pdf

***Andres R. Almanza J., Ms.C, CISM**. Coach Ejecutivo y Chief Growth Officer en CISOS.CLUB. Ingeniero de Sistemas y Computación de la Universidad Católica de Colombia. Especialista en Seguridad en Redes de la Universidad Católica de Colombia. Máster en Seguridad Informática, Ms.C, de la Universidad Oberta de Cataluña, España. Profesional certificado como Coach Ejecutivo y de Vida, por la International Coaching Leadership and Future Achivement. Profesional certificado como Information Security Manager (CISM), por ISACA. Docente de Cátedra de la Universidad Externado de Colombia. Miembro del Comité Editorial de la Revista "Sistemas" de la Asociación Colombiana de Ingenieros de Sistemas (ACIS).*

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.*

El profesional de seguridad de la información

Un análisis de su evolución: 1960-2030+

DOI: 10.29236/sistemas.n147a6

Resumen

La rápida evolución del entorno de negocios y el advenimiento de otra revolución industrial revelan nuevos retos para el área de seguridad de la información. En este sentido, analizar el desarrollo de esta área a lo largo del tiempo, permite observar los desafíos para los profesionales de seguridad de la información en un contexto gobernado por la inestabilidad y la incertidumbre. Por tanto, este documento busca reflexionar sobre las variaciones en sus competencias y proyectar el ejercicio de una práctica de protección, consolidada con los requerimientos de las organizaciones y los negocios del siglo XXI.

Palabras clave

Seguridad de la información, perfil, capacidades, prácticas, ciber

Jeimy J. Cano M.

Introducción

Entender la evolución de los profesionales de seguridad de la información y los retos que vienen en el mediano y largo plazo, es comprender el nuevo entorno de las organizaciones. En la medida en que las compañías cambian y se reinventan, el área de seguridad se articula para proteger la promesa de valor de la empresa.

Es claro que, ante una mayor conectividad e interacción entre individuos y las máquinas, mayores se-

rán los retos que el área de seguridad de la información deba enfrentar. En este contexto, las habilidades y saberes de sus profesionales, deberán ser ajustados y reinventados, para dar cuenta de la complejidad que supone un entorno digitalmente modificado, en el que la inseguridad de la información puede camuflarse de diferentes formas.

Así las cosas, revisar cómo ha evolucionado la función de seguridad de la información establece un escenario de análisis de los retos, que tanto el ejecutivo del área, como su equipo de trabajo deben entender, asumir y superar, para construir una hoja de ruta de reinvención de sus puestos de trabajo, para acompañar a los negocios y navegar en medio de tensiones y tormentas inesperadas que puedan y quieran comprometer la promesa de valor de la empresa.

En este contexto, se revisa la evolución del perfil del profesional de seguridad de la información, de la mano con la evolución del área de seguridad de la información, analizando en cada uno de sus momentos, los focos estratégicos de su gestión y los retos que implica el entorno digital, tecnológicamente modificado, móvil e hiperconectado de forma acelerada y con sobrecarga de información.

Seguridad de la información: una perspectiva evolutiva del área y sus perfiles

1960-1970 – Controles tecnológicos

Una primera fase de la evolución inicia en los años 60 y 70, cuando la seguridad de la información estaba concentrada en el ***desarrollo y aplicación de acciones tecnológicas basadas en el control de acceso***, las cuales permanecen en la actualidad. Este desarrollo técnico ubicaba a la función de seguridad en las áreas de tecnologías de información y comunicaciones, asociada con los especialistas del tema, que conocían bien la manera de configurar dichos controles para asegurar el acceso de las personas a la información y la ejecución de sus programas autorizados (Department of Defense, 1970).

Esta vista eminentemente tecnológica convierte a los profesionales de seguridad de la información en especialistas con lenguaje técnico y estudios profundos en ciencias de la computación. La esencia de la práctica de estos profesionales era conocer en detalle los controles, su diseño, efectividad y la manera de efectuar seguimiento a su implementación. Sus reflexiones y aportes buscan disminuir la exposición de la empresa a las amenazas del momento y proteger el acceso a la información.

1980-1990: Riesgos y procesos

Con la llegada de internet, durante los años 80 y 90, la seguridad de la información se observa desde ***la vista de procesos y riesgos***, es decir, la comprensión de la inevita-

bilidad de la falla se incorpora en la dinámica de las actividades de la empresa, ubicando a la información en un lugar visible y con impactos particularmente claves, motivando reflexiones adicionales que sacan a la seguridad de un lindero eminentemente tecnológico, para leerlo a la luz de los resultados propios de la realización de las funciones del negocio.

Ahora no es solamente qué tan bien está configurado el control de acceso, sino comprender los impactos de una gestión inadecuada de los riesgos identificados en los procesos, lo cual ubica al área de seguridad en la lectura de los dominios de los sistemas de gestión y de riesgo empresariales.

En este escenario, los profesionales de seguridad de la información no solamente tienen un lenguaje tecnológico, sino de procesos. Sus perspectivas y reflexiones contemplan nuevos saberes desde la realidad de las actividades del negocio, reconociendo cómo la información fluye y permite que se alcancen los objetivos empresariales.

2000-2010: Cumplimiento y objetivos estratégicos

Entrado el nuevo milenio y su primera década, el tema de la seguridad y control evoluciona hacia un lugar más corporativo. Ahora se incorpora dentro de las ***exigencias de cumplimiento regulatorio***, como quiera que el ejercicio empresarial en el contexto de una sociedad de la información y el conocimiento, demanda una serie de condiciones básicas para aumentar la confianza de los clientes y proteger el valor de los inversionistas. La proliferación de normas con exigencias de protección y aseguramiento de información, elevan la discusión de la seguridad al escenario de satisfacer requerimientos por los cuales las empresas pueden o no pertenecer a un grupo particular (por ejemplo, la OCDE –Organización para la Cooperación y el Desarrollo Económico–) o cotizar en bolsas de valores nacionales e internacionales (p.e. la bolsa de valores de New York, en los Estados Unidos de América).

En este sentido, no son sólo los controles tecnológicos y la gestión del riesgo sobre el inadecuado tratamiento de la información, sino ahora se trata de las sanciones que imponen los reguladores por incumplimientos de las normas y estándares que generan confianza a los terceros interesados, llevando a la función de seguridad a los dominios de las áreas de cumplimiento.

Los profesionales de seguridad de la información de este momento, deben ser hábiles lectores e intérpretes de las normas de cumplimiento nacional e internacional, que articuladas con las prácticas vigentes, tanto en controles tecnológicos como de riesgos empresariales, sean capaces de enviar un mensaje claro a los ejecutivos sobre sus deberes de cumplimiento

normativo para darle profundidad a la naciente cultura organizacional de seguridad de la información (Cano, 2016), ahora vista desde el ejercicio de buenas prácticas de protección de la información y aseguramiento de los procesos.

2020-2030+: Ecosistema digital

Con la modificación acelerada del mundo a través de la tecnología y en el marco de una sociedad digitalmente modificada hacia 2020, en la que el flujo de información se percibe con mayor claridad en los ***nuevos productos y servicios de las "cosas conectadas"***, se observa una nueva revolución industrial que, en forma instantánea, permite obtener información sobre el estado de las cosas y las personas. Una realidad que experimenta cambios y se ajusta conforme las personas actúan y se relacionan con otras.

En este escenario, la seguridad de la información se convierte en un valor fundamental, en una exigencia necesaria y obligatoria que permite a las personas mantenerse conectadas con la tranquilidad de que su "realidad digital", representada en todo lo que recibe y transmite, se mantiene dentro del dominio de experiencia que ellas han declarado compartir (Porter y Heppelmann, 2015).

Así las cosas, la protección de la información no sólo se traduce en medidas tecnológicas dentro de la organización, orientadas por una gestión de riesgos y controles propios de los procesos, que asisten las exigencias de cumplimiento normativo nacionales e internacionales, sino que ahora deben concretar elementos de protección más allá de los límites empresariales y asegurar que los productos y servicios que consumen sus clientes funcionen de tal manera, que no permitan que una falla de los mismos, comprometa o afecte la esfera personal y familiar de sus usuarios. Por tanto, se pasa de una distinción de protección de afectaciones que vienen del exterior a mantener una operación interna de productos y servicios confiable, que funcione y sobreviva a pesar de los ataques externos (Bughin, Lund y Manyika, 2016).

En consecuencia, la función de seguridad de la información adquiere mayor visibilidad y sensibilidad por parte de los clientes y, por tanto, entre los ejecutivos de la empresa, generando mayor necesidad de conocimiento de los avances y prácticas de protección dentro de la operación de la compañía, como en los procesos de producción y fabricación de los productos y servicios, habida cuenta de que una falla generalizada en uno de ellos, no sólo tiene alcances técnicos, sino repercusiones económicas, sociales, políticas y administrativas. En pocas palabras, se evidencian las relaciones sistémicas que la empresa mantiene con su entorno y cómo éste afecta la manera en que la compañía desarrolla su actividad económica (De Geus, 2011).

Bajo este escenario, la función de seguridad y control se especifica a través de lo que se denomina riesgo "ciber", una categoría que no sólo concreta lo tecnológico como tal, sino la integración o convergencia entre lo físico y lo lógico, que cambia la forma como se configura la relación entre la empresa y los clientes, así como la manera en que se conciben los impactos dentro y fuera de la organización. Lo "ciber" conecta a la empresa en un espacio de relaciones hacia el exterior, para entender cómo sus operaciones afectan a otros y cómo los otros y sus actividades concretan efectos en su desarrollo de negocio, es decir, un ecosistema digital (Frappolli, 2015).

Luego, la función de seguridad de la información modifica su postura de cumplimiento normativo, por una lectura de valor para el negocio, de implicaciones políticas para los miembros del directorio, de impactos en las expectativas de los clientes y, sobre manera, en la supervivencia de la empresa en un entorno digital.

Con esta lectura, el ejecutivo de seguridad deberá madurar y desarrollar un discurso políticamente correcto, que, asistido por su conocimiento del entorno, como buen estratega que debe ser, ilustra la forma para superar el laberinto de las amenazas emergentes, comprometiendo las voluntades de los directores de la junta para concebir una lectura conjunta de la estrategia corporativa digitalmente responsable (Cano, 2015; Choudhary, 2015).

Por tanto, un profesional de seguridad de la información competente en un mundo como el propuesto, siguiendo las reflexiones de Echeverría et al (2014, p.77) "*no puede reducirse ni a un saber específico ni a una capacidad específica. La competencia exige pasar del saber hacer al saber actuar, ir más allá de lo prescrito*".

Lo anterior en perspectiva sistémica, significa comprender la seguridad de la información como un "*darnos cuenta de nuevas posibilidades… lo que implica cuestionarse los supuestos, significados, valores y normas que generalmente damos por sentados*" (Espejo y Reyes, 2016, p.63), con el fin de hacer nuevas distinciones que se conviertan en acciones prácticas incorporadas, las cuales no sólo permiten construir el mundo y desempeñarse en él, sino actuar como profesionales únicos y particulares (ídem, p.64).

En consecuencia, como afirma Echeverría (2014 et al, p.78) "*el profesional competente se caracteriza predominantemente por saber innovar, más que por los saberes rutinarios. Es decir, por poner en práctica conductas y actos pertinentes en situaciones inéditas*". Esto es, en la lectura sistémica, un entendimiento de la seguridad de la información en un contexto particular

que revela una red de interacciones, para hacer frente a los desbalances de complejidad propios de aquella, rediseñando las prácticas actuales o clasificando y agrupando las inestabilidades de la situación observada (Espejo y Reyes, 2016).

En tal sentido, la función de seguridad de la información no estará atada a las connotaciones técnicas de los dispositivos tecnológicos ni a las normas o riesgos particulares de las plataformas, sino a las lecturas ejecutivas que definen el futuro de las empresas. Las discontinuidades del entorno, particularmente basadas en estrategias digitales, se transforman en eventos relevantes que alteran la realidad empresarial y que son leídos por los miembros de la junta como eventos para revisar alrededor de las oportunidades o amenazas, en las que el ejecutivo de seguridad y control, forma parte de la vista valiosa que define el posicionamiento de la empresa entre los clientes (Kaplan, Bailey, O'Halloran, Marcus & Rezek, 2015; Veltos, 2016).

Reflexiones finales

Revisar la evolución del área de seguridad de la información, desde el mundo de los controles de tecnología, hasta su visión digitalmente modificada, en la cual las relaciones y sus impactos son evidentes; se trata de caminar por un sendero retador de aprendizaje/desaprendizaje para los profesionales de seguridad de la información en el que, como anota Morin (2011), abundan las incertidumbres con algunos pocos archipiélagos de certezas.

Es un proceso en el que se cambia un aprendizaje mecanicista fundado en repetir una fórmula probada y validada en un entorno medianamente conocido y cierto, a uno sistémico, sensible al contexto, en el que diferentes interacciones de los actores del escenario pueden cambiar las condiciones de operación de los productos y servicios de las empresas. En este sentido, los profesionales de seguridad de la información deben incorporar prácticas y reflexiones claves que les permitan equivocarse rápido, capitalizar lecciones aprendidas, generar controversias y vencer sus sesgos cognitivos, de tal forma que puedan anticipar riesgos y amenazas emergentes que afecten los nuevos activos digitales de las empresas.

En pocas palabras, lo anterior significa ejercer un “CiberLideraXgo” digitalmente confiable, que les permita:

- *Actuar de forma rápida*. Caminar con los retos empresariales y contar con los escenarios dispuestos para experimentar y simular soluciones de forma ágil y efectiva. Equivocarse es una virtud y no un defecto. Aprender rápido, es superar las barreras cognitivas de aquello que se conoce para tomar riesgos de forma inteligente.

- *Experimentar mucho*. Contar con entornos psicológicamente seguros, donde la contradicción y la experimentación sean parte natural de las reflexiones. Aprender, desaprender, desconectar y reconectar, son palabras que definen la manera como el profesional de seguridad de la información conoce y descubre su propio entorno y la realidad de los negocios.
- *Adoptar de forma temprana*. Utilizar plataformas y ecosistemas de despliegue rápido, con terceros de confianza, que permitan concretar grupos de pruebas, con el fin de desarrollar y consolidar las nuevas competencias digitales requeridas para articular los retos empresariales con las nuevas experiencias de los clientes.

- *Reinventar siempre*. Anticipar tendencias, comprender los riesgos y amenazas digitales inherentes al entorno digital y tecnológicamente modificado, con el fin de defender la promesa de valor para los clientes, consolidando acciones encaminadas a asegurar una confianza digital que proporcione profundidad y transparencia a los productos y/o servicios entregados a los consumidores.

En resumen, el profesional de seguridad de la información deberá ser una persona que construye relaciones de largo plazo, que crece con las organizaciones, creando espacios como afirmaba Steve Jobs, "*donde las ideas ganen las discusiones, no las jerarquías*". Un ejercicio de disciplina, colaboración y confianza que erige puentes para deconstruir el pasado, reinventar el presente y hacer realidad el futuro; es decir, una transformación de prácticas que buscan inicialmente proteger y asegurar la información clave de una empresa, para construir capacidades orientadas a defender y anticipar los retos y las amenazas emergentes, como una manera de custodiar la promesa de valor de las empresas.

Referencias

Bughin, J., Lund, S. & Manyika, J. (2016) Five priorities for competing in an era of digital globalization. Mckinsey Quarterly. Mayo. Recuperado de: http://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/five-priorities-for-competing-in-an-era-of-digital-globalization

Cano, J. (2015) Juntas directivas. Descifrar e influenciar su imaginario vigente sobre la seguridad de la información. *Blog IT-Insecurity*. Recuperado de: http://insecurityit.blogspot.com.co/2015/08/juntas-directivas-descifrar-e.html

Cano, J. (2016) Modelo de madurez de cultura organizacional de seguridad de la información. Una visión desde el pensamiento sistémico-cibernético. *Actas XIV Reunión Española sobre Criptología y Seguridad de la Información*. ISBN: 978-84-608-9470-4. Octubre. pp 24-29.

Choudhary, U. (2015) This Might Be The Next Coveted Leadership Position Of 2015. *F@stcompany Magazine.* Recuperado de: https://www.fastcompany.com/3043376/how-to-earn-respect-from-the-hottest-seat-in-leadership-today

De Geus, A. (2011) *La empresa viviente. Hábitos para sobrevivir en un ambiente de negocios turbulento*. Buenos Aires, Argentina: Editorial Gránica.

Department of Defense (1970) Security controls for computer systems (U). *Report of Defense Science Board Task Force on Computer Security*. Febrero. Recuperado de: http://seclab.cs.ucdavis.edu/projects/history/papers/ware70.pdf

Echeverría, B. (Coordinador), Isus, S. Martínez, M. P. y Sarasola, L. (2014) *Orientación profesional*. Segunda reimpresión. Barcelona, España: Editorial UOC.

Espejo, R. y Reyes, A. (2016) *Sistemas organizacionales. El manejo de la complejidad con el modelo del sistema viable*. Bogotá, Colombia: Ediciones Uniandes–Universidad de Ibagué.

Frappolli, M. (2015) *Managing cyber risk*. Malvern, Pennsylvania.USA: American Institute for Chartered Property Casualty Underwriters. https://www.fastcompany.com/3043376/how-to-earn-respect-from-the-hottest-seat-in-leadership-today

Kaplan, J., Bailey, T., O'Halloran, D., Marcus, A. y Rezek, C. (2015) *Beyond cybersecurity. Protecting your digital business*. Hoboken, New Jersey. USA: Editorial John Wiley & Sons.

Morin, E. (2011) *Los siete saberes necesarios para la educación del futuro*. Madrid, España: Editorial Paidós.

Porter, M. y Heppelmann, J. (2015) How Smart, connected products are transforming companies. *Harvard Business Review*. Octubre.

Veltsos, C. (2016) Is Your CISO Out of Place? *IBM Security Intelligence*. Recuperado de: https://securityintelligence.com/is-your-ciso-out-of-place/

***Jeimy J. Cano M., Ph.D, CFE**. Profesor Asociado. Escuela de Administración, Universidad del Rosario. Ingeniero y Magíster en Ingeniería de Sistemas y Computación de la Universidad de los Andes. Especialista en Derecho Disciplinario de la Universidad Externado de Colombia. Ph.D in Business Administration por Newport University, CA. USA. Profesional certificado como Certified Fraud Examiner (CFE), por la Association of Certified Fraud Examiners. Director de la Revista Sistemas de la Asociación Colombiana de Ingenieros de Sistemas –ACIS–.*

FORTINET®

GAMMA® INGENIEROS

Las amenazas evolucionan al ritmo de la tecnología.

Integramos inteligencia a su estrategia de seguridad.

CONTÁCTENOS

USUARIO | ENDPOINT | CONECTIVIDAD | SERVICIOS Y APLICACIONES | CIBERDEFENSA

Expertos en Ciberseguridad e Infraestructura Tecnológica.

Gamma Ingenieros Colombia | Gamma Ingenieros | Gamma Ingenieros

www.gammaingenieros.com

globaltek
SECURITY

1995 - 2018

Cumplimos 23 años de experiencia en la ejecución de proyectos de Seguridad de la Información y protección de activos digitales

Numerosas organizaciones del sector público y privado en Colombia y en Latinoamérica, han confiado en el profesionalismo y suficiencia técnica que Globaltek Security ha demostrado a través de los años, que la cataloga como una compañía estructurada y bien preparada para el desarrollo de proyectos e implementación de servicios orientados a la Seguridad de la Información, protección de activos digitales y datos sensibles de la organización.

Contáctenos: info@globalteksecurity.com
Gerencia Comercial – Pedro Muñoz
pedro.munoz@globalteksecurity.com
Celular 310 232 1344

GLOBALTEK SECURITY es SEGURIDAD DE LA INFORMACION.