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.*