

¿Expertos, Especialistas o Profesionales en inseguridad informática?

Por

Jeimy J. Cano, Ph.D, CFE

Profesor- Investigador

GECTI

Universidad de los Andes

Es frecuente escuchar los términos “experto en seguridad informática”, “especialista en seguridad informática” o “profesional en seguridad informática”, tres palabras, tres contextos que nos deben animar a una reflexión personal y profesional alrededor de aquellos interesados que enfrentan día a día los retos de la inseguridad informática. (HOWARD 2008, BRATUS 2007)

De acuerdo con el diccionario de la Real Academia Española - RAE, existen diferencias importantes entre las tres palabras: experto, especialista y profesional.

Para la RAE un *experto*, viene del latín *expertus*, alguien experimentado en algo, alguien que ha probado o tratado con algo. Se asocia generalmente a un perito. Un *especialista*, es alguien que cultiva o practica una rama determinada de un arte o una ciencia, de la que tiene particulares conocimientos y habilidades. Finalmente un *profesional*, es una persona que ejerce su profesión con relevante capacidad y aplicación.

Mirando estas tres definiciones se puede sugerir que los que se dedican a la seguridad informática (o inseguridad de la información), siendo estrictos en el manejo de las anteriores, responden a un proceso evolutivo que los cautiva y los lleva a explorar su propia curiosidad con eventos que desafían lo establecido, para generar nuevas inquietudes y así, continuar aprendiendo. Es un proceso de desaprendizaje (POURDEHNAD, J., WARREN, B., WRIGHT, M. y MAIRANO, J. 2006) que invita a reconocer que no sabemos y que debemos estar atentos a descubrir las nuevas propuestas que nos ofrece el evento que se estudia.

Un experto en seguridad informática, siguiendo lo sugerido por la real academia, es alguien que se ha enfrentado a la inseguridad de la información, alguien que se ha enfrentado a la incertidumbre que genera la falla, a la presión que se manifiesta en ese momento para tomar acciones que ponen a prueba su conocimiento y experiencia previa en situaciones semejantes (nunca iguales). Las acciones acertadas o no, son el insumo de las futuras que esta persona enfrente, cuando nuevamente sea sorprendida por un nuevo episodio de la inseguridad informática.

Con el paso del tiempo este experto, desarrolla un instinto o intuición en el arte de conocer y descubrir la inseguridad; en ese momento se transforma en un especialista, no de seguridad informática, sino de inseguridad de la información. El enfrentamiento constante con la inseguridad y la falla, genera en este personaje una mente más abierta y sistémica, más llevada por las relaciones y efectos emergentes, que por eventos puntales. El

especialista estructura una red de conocimientos y prácticas que proponen soluciones emergentes, generalmente diferentes y alternas a las que pudiesen ofrecer lo que dicen las buenas prácticas actuales. Recordemos que las buenas prácticas, nacen del reconocimiento de acciones que han demostrado ser útiles en el tiempo.

Finalmente el profesional en seguridad informática, sería una persona que ejerce una profesión, un oficio, que generalmente se encuentra estructurado bajo una serie de lineamientos y conceptos que son avalados y normados por entes reguladores en temas académicos o científicos. De esta forma, existen las profesiones como la ingeniería, el derecho, la medicina, entre otras.

En este contexto y considerando que a la fecha no existe un acuerdo nacional o internacional sobre currículos en seguridad de la información, tratar de responder la pregunta *¿qué debo estudiar para aprender seguridad informática?* es un reto que aún tenemos que enfrentar y donde tenemos grandes oportunidades para proponer y avanzar.

El profesional en seguridad informática actualmente es tema de discusión y análisis en diversos foros internacionales. Iniciativas como las efectuadas en la Universidad Politécnica de Madrid, orientada por el Dr. Jorge Ramio Aguirre (ver <http://www.criptored.upm.es>, sección docencia), las consideraciones de formación en seguridad informática (particularmente orientadas al desarrollo de software seguro) sugeridas por el Dr. Matthew Bishop (<http://nob.cs.ucdavis.edu/bishop/papers/>), de la Universidad de California, en Davis, entre otras iniciativas (ver otras fuentes adicionales) son elementos que nos dicen que debemos continuar analizando posibilidades y estrategias para acercarnos cada vez más a un acuerdo base sobre lo que un profesional de seguridad informática debería estudiar.

Por otro lado se encuentran las certificaciones en seguridad informática (JOSS 2003), que si bien son esfuerzos importantes adelantados por la industria, para establecer referentes de formación en temas de seguridad informática, no corresponden formalmente a una estrategia académica y científica, que exija del profesional investigación profunda y aplicada, así como generación de conocimiento. Las certificaciones son un complemento a la formación académica, que definitivamente son apreciadas en los entornos laborales, dado que la academia aún se encuentra definiendo lo que debería ser la formación de un profesional en seguridad de la información.

La seguridad informática en su evolución desde los años 50's, ha venido mostrando patrones característicos e inquietudes particulares, generalmente atadas con la evolución de la inseguridad de la información. Si bien, cada vez que evolucionan las plataformas tecnológicas, la inseguridad se transforma, es importante observar que los profesionales de seguridad no lo hacen de la misma manera, pues, deben recorrer nuevamente la curva de aprendizaje que les exige el nuevo contexto computacional o de negocio que se enfrenta.

En razón a lo anterior y no obstante, los aspectos evolutivos de las tecnologías de información (CANO 2008, CANO 2008b), si se requiere adelantar un ejercicio de exploración y análisis sobre las prácticas de seguridad y los patrones que sugiere la inseguridad para delinear un **perfil evolutivo de aprendizaje de la seguridad**, que

considere la exposición de los interesados sobre temas conocidos en seguridad, para avanzar y conocer comportamientos desconocidos ocasionados por la inseguridad. Esto permite disminuir el riesgo de que el experto (siguiendo la definición de RAE) sea víctima de “una falsa sensación de seguridad” y mantenga un mínimo de paranoia, requerida para mantenerse vigilante.

Si mantenemos a este experto, en proceso evolutivo de desaprendizaje, es decir, confrontando las buenas prácticas, los mecanismos de seguridad y sus procesos de construcción y afinamiento, inspeccionando código en búsqueda de funciones inseguras, analizando comportamientos adversos de personas en las organizaciones, entre otros elementos, pronto tendremos un especialista que de manera sistémica (KEILY, L y BENZEL, T. 2006) observe y diagnostique una situación antes de que ocurra. Si bien, no podrá anticiparse a todo lo que puede ocurrir, si estará atento a nuevas relaciones que la inseguridad pueda sugerir.

Como hemos visto hasta el momento y sabiendo que la inseguridad de la información es un “camino que se revela al andar”, las personas que se dedican a la seguridad de la información, bien sean expertas, especialistas o profesionales siempre tendrán algo en común, una misión y deseo que los marca, una convicción de vida personal y profesional que los une: el reto de conocer, descubrir y aprender de la inseguridad de la información.

Referencias

- BRATUS, D. (2007) What hackers learn that the rest of us don't. Notes on hacker curriculum. *IEEE Security & Privacy*. July-August. PP.72-75
- CANO, J. (2008) La evolución de la inseguridad informática: Una visión tecnológica. Parte 1. *ComputerWorld*. Enero.
- CANO, J. (2008b) La evolución de la inseguridad informática: Una visión tecnológica. Parte 2. *ComputerWorld*. Febrero.
- HOWARD, M. (2008) Becoming a security expert. *IEEE Security & Privacy*. January-February. PP. 71-73
- JOSS, M. (2003) Certifications are essential for all IT security staffers. Disponible en: <http://news.zdnet.co.uk/itmanagement/0,1000000308,2132282,00.htm>
- KEILY, L y BENZEL, T. (2006) Systemic security management. *IEEE Security & Privacy*. Noviembre-Diciembre.
- POURDEHNAD, J., WARREN, B., WRIGHT, M. y MAIRANO, J. (2006) Unlearning/Learning Organizations – The Role of Mindset. *Proceedings of 50th International Society of Systems Science Conference*. Disponible en: http://www.iss.org/conferences/sonoma2006/2006_ISSS_50thAnnualMeeting_Sonoma_Program-Body-Acrobat6-150dpi.pdf

Otras Fuentes adicionales:

- * NSTSC (2003) National Strategy to Secure Cyberspace. A National Cyberspace Security Awareness and Training Program. p. 37 Available on March. 12, 2004. http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf
- * Information Security (Master of Science in Information Security Technology and Management - MSISTM). 13 Jan 2003. Carnegie Mellon University. Available on March 12, 2004 at <http://www.ini.cmu.edu/academics/MSISTM/index.htm>

* Master of Science in Computer Science Concentration in Information Security. James Madison University. Available on March 12, 2004 at <http://www.infosec.jmu.edu/website/overview.htm>

* Infosec Graduate Program. Purdue University. Available on March 12, 2004 at http://www.cerias.purdue.edu/education/graduate_program/

* Master of Science in Security Informatics. Johns Hopkins University. Available on March 12, 2004 at <http://www.jhuisi.jhu.edu/education/index.html>

* Master of Science degree program in Information Security and Assurance. George Mason University. Available on March 12, 2004 at <http://www.isse.gmu.edu/ms-isa/>

* Dark, Melissa. Davis, Jim. "Report on Information Assurance Curriculum Development". The Center for Education and Research in Information Assurance and Security (CERIAS). Available on March 12, 2004 at http://www.cerias.purdue.edu/education/post_secondary_education/undergrad_and_grd/curriculum_development/information_assurance/

Datos del Autor:

Jeimy J. Cano, Ph.D, CFE

Miembro investigador del Grupo de Estudios en Comercio Electrónico, Telecomunicaciones e Informática (GECTI). Facultad de Derecho. Universidad de los Andes. Colombia. Miembro Investigador de ALFA-REDI (Red Latinoamericana de Especialistas en Derecho Informático). Ingeniero de Sistemas y Computación, Universidad de los Andes. Magíster en Ingeniería de Sistemas y Computación, Universidad de los Andes. Ph.D in Business Administration, Newport University. Profesional certificado en Computer Forensic Analysis (CFA) del World Institute for Security Enhancement, USA. Profesional certificado como Certified Fraud Examiner (CFE) por la Association of Certified Fraud Examiners. Contacto: jjcano@yahoo.com