Cómo convertirse de un practicante a un profesional de la seguridad de la información

Kerry Anderson, CISA, CISM, CRISC, CGEIT, CCSA, CFE, CISSP, CSSLP, ISSAP, ISSMP, se desempeña como consultora de gestión de seguridad de la información y de registros electrónicos, y reúne una experiencia de más de 15 años en materia de seguridad de la información. Ha disertado en numerosos eventos y escrito diversos artículos en publicaciones específicas del sector. Es profesora adjunta en el Curso de Posgrado sobre Seguridad Cibernética que se dicta en Clark University (Worcester, Massachusetts, EE. UU.).

"Yo soy un practicante en seguridad de la información; no soy un profesional". Hay una enorme diferencia entre ambos conceptos. Un practicante es "alguien que ejerce o practica una actividad, especialmente una ocupación, profesión o técnica". Un profesional se define como "un practicante con excelentes habilidades y destrezas; un experto".[1] Los elementos diferenciadores de estos dos términos son, básicamente, el grado de experiencia y el nivel de conocimiento. En una situación ideal, los practicantes deberían avanzar de un nivel al otro una vez adquirida la pericia necesaria para desempeñar cada puesto o función que se les asigne. Lamentablemente, el desarrollo de competencias fundamentales no suele ser un proceso lineal. Adquirir la pericia necesaria para cumplir con los objetivos de carrera deseados puede exigir un esfuerzo proactivo del practicante.

Para forjarse una carrera en el campo de la seguridad de la información, los practicantes deben adquirir competencias fundamentales en áreas específicas. Las competencias fundamentales de una profesión conforman el modelo de competencias aplicables. Ese modelo de competencias y los esfuerzos realizados para adquirirlas son los factores que distinguen a un novato de un experto en una profesión. La adquisición de competencias fundamentales es esencial para avanzar al siguiente nivel. Y aunque esto parezca obvio, posiblemente sea más difícil de lograr ante la creciente especialización observada en el campo de la seguridad de la información.

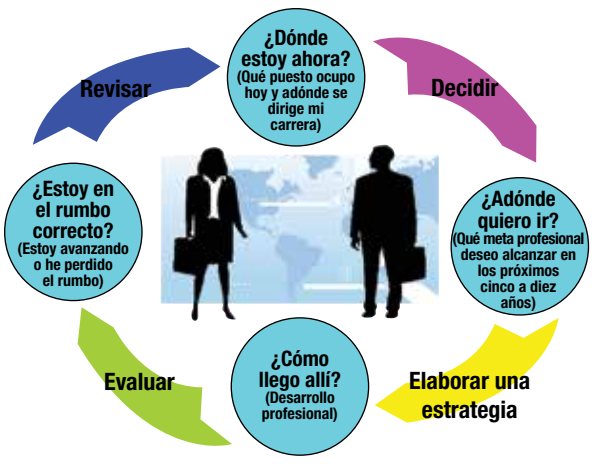
Un practicante de la seguridad de la información debe adquirir las competencias fundamentales para desarrollar una perspectiva integral, que le permita gestionar con eficacia la seguridad en un mundo globalizado y sumamente interconectado, como el de hoy. Estas competencias se desarrollan en distintas etapas de la carrera y comprenden no solo el conocimiento técnico, sino otras habilidades necesarias para convertirse en un profesional competente. Las nuevas especializaciones en seguridad de la información demandan sólidas competencias en áreas fundamentales para gestionar arquitecturas cada vez más complejas, pero también exigen la adquisición de nuevas competencias para no perder relevancia.

MAPA DE COMPETENCIAS FUNDAMENTALES

Un mapa es un excelente modelo para el desarrollo profesional, ya que proporciona mecanismos para fijar un rumbo y para realizar los ajustes necesarios en caso de que surja algún imprevisto. Un mapa hipotético de competencias fundamentales (**figura 1**) consta de cuatro pasos.

Este proceso es reiterativo por dos motivos. En primer lugar, la seguridad de la información existe dentro de un entorno tecnológico

Figura 1: Mapa de competencias fundamentales



dinámico; por tanto, es indispensable renovar habilidades para no quedar totalmente desactualizado a nivel profesional. Por ejemplo, muchas de las carreras que hoy tiene gran demanda, como la de ingeniería en seguridad en la nube, no existían hace algunos años. El segundo motivo consiste en que el practicante también existe dentro de un entorno dinámico. Muchas veces es necesario encauzar la carrera en función de los cambios producidos en las circunstancias, los intereses o las ambiciones personales. Durante los últimos años, muchos practicantes se vieron en la necesidad de hacer reajustes en sus carreras profesionales.[2]

PASO 1: IDENTIFICAR LA POSICIÓN ACTUAL EN LA TRAYECTORIA PROFESIONAL

El proceso comienza con la identificación de la posición que uno está ocupando en su carrera profesional. La premisa básica consiste en que las personas necesitan saber dónde están ahora para idear el modo de alcanzar la meta prevista. Es indispensable realizar una evaluación de los niveles de competencia. Quienes están dando sus primeros pasos en el campo de la seguridad podrían identificar estos niveles claramente, pero a las personas que poseen más experiencia o desean realizar un cambio en sus carreras probablemente les cueste más determinar qué competencias fundamentales dominan y cómo las dominan.

PASO 2: ESTABLECER UN OBJETIVO PROFESIONAL A MEDIANO Y LARGO PLAZO

Es preciso determinar el rumbo que uno quisiera seguir en los próximos cinco a diez años, tomándose un tiempo para reflexionar detenidamente sobre una serie de preguntas vinculadas a los intereses, el temperamento personal y los desafíos profesionales que uno desea enfrentar. Este paso generalmente exige una investigación de las opciones disponibles a nivel profesional, entre ellas:

Figura 2: Areas de pericia en seguridad de la información

Area	Explicación
Tecnología aplicada a la seguridad	Esta área de pericia incluye conocimiento, habilidades y experiencia en relación con la tecnología aplicada a la seguridad de la información. El nivel inicial se centra en el desarrollo de una mayor comprensión del tema, con especial hincapié en la competencia técnica. En los niveles más avanzados, las experiencias y habilidades deben alcanzar grados de pericia específicos, como gestión de accesos, criptografía, gestión operacional, desarrollo de aplicaciones, arquitectura de seguridad, comunicación (voz/datos), personal, y seguridad física y ambiental.
Gestión de personas	Esta área de pericia incluye conocimientos, habilidades y experiencias relacionadas con la comunicación eficaz de información, y con las técnicas de persuasión, influencia y negociación para la celebración de acuerdos en todos los niveles de una organización. La pericia en esta área comprende las habilidades de comunicación escritas y verbales. Todos los practicantes deben desarrollar habilidades sociales para comunicar sus ideas, promover la visibilidad personal, mejorar las relaciones, generar apoyo para las iniciativas y estimular cambios de conducta para desarrollar una cultura de seguridad dentro de la organización.
Gestión de riesgos	Esta área de pericia abarca la comprensión, el desarrollo y la gestión de un enfoque basado en los riesgos para abordar los programas de seguridad de la información. Incluye la pericia para la identificación, evaluación y remediación de riesgos, las vulnerabilidades y amenazas. Las habilidades en esta área abarcan el análisis de riesgo y la identificación de potenciales controles para mitigar el riesgo identificado. En el nivel inicial, la gestión de riesgos es el foco interno. En los niveles más altos, el practicante incorpora preocupaciones relacionadas con los riesgos externos, a los vectores de riesgo de tecnologías emergentes y a las relaciones con terceros.
Tecnología de la información	Esta área de pericia incluye conocimientos, experiencia y habilidades relacionadas con el desarrollo, las pruebas, la implementación, la gestión y el retiro de aplicaciones y su infraestructura técnica de soporte. La competencia en este campo abarca el desarrollo de conocimientos prácticos en hardware, software y redes, así como en sus interrelaciones. En los niveles inferiores de pericia, las habilidades de TI se desarrollan en torno a tecnologías específicas y a operaciones. En los niveles más altos, el nivel y alcance de las habilidades se extiende a varias áreas de TI con especial atención en la integración y la gestión de riesgos.
Gestión de seguridad de la información	Esta pericia implica una cabal comprensión de la teoría, los principios, las metodologías, el cumplimiento y el gobierno de la seguridad. Proporciona el eslabón que conecta a la tecnología con las funciones de negocio requeridas para gestionar el riesgo inherente de la seguridad en la organización. Se requiere capacitación y experiencia para aplicar un proceso de gestión de seguridad en situaciones reales. Es en este ámbito donde muchos practicantes realizan la transición y se convierten en profesionales de la seguridad de la información. En el nivel inicial, los practicantes pueden aplicar técnicas debidamente documentadas para gestionar los factores comunes de riesgo. Los profesionales con mayor pericia desarrollan o adaptan técnicas de gestión de seguridad de la información a tecnologías emergentes o a un conjunto de circunstancias únicas.

- Entrevistas para reunir información
- Proyecciones laborales
- Predicciones de las tendencias en el mercado laboral
- Encuestas sobre puestos de trabajo para determinar los requisitos usuales de esos cargos

PASO 3: DESARROLLAR UN PLAN

Este paso comprende dos tareas. La primera consiste en determinar el conjunto de habilidades y experiencia que uno posee. La siguiente es desarrollar una estrategia que permita obtener la pericia necesaria para alcanzar un objetivo profesional. La finalidad es estar preparados para aprovechar las oportunidades laborales que surjan. Tal como decía Benjamin Disraeli: "Uno de los secretos del éxito en la vida es estar preparado para cuando se presente la oportunidad".[3]

Tarea 1: Evaluar la pericia

Esta tarea consiste en comparar los niveles de competencia con la pericia requerida para subir un escalón en la carrera profesional. La discrepancia entre las habilidades y niveles de conocimiento existentes y el nivel de pericia sugerido representa una brecha en la competencia dentro de un área. Una estrategia sencilla para medir la pericia podría consistir en el cálculo de los años de experiencia para realizar una clasificación en cuatro categorías:[4]

- **Practicante de nivel inicial:** tres años (o menos) de experiencia en seguridad de la información.
- **Practicante de nivel medio:** de cuatro a siete años de experiencia en seguridad de la información.
- **Practicante de nivel superior:** de ocho a diez años de experiencia en seguridad de la información.
- **Profesional de nivel ejecutivo/experto:** más de diez años de experiencia en seguridad de la información.

Estos niveles indican el grado de habilidad o experiencia que posee un practicante en relación con un campo específico. También representan una escala de responsabilidades diferentes desde el nivel inicial del practicante hasta el del profesional ejecutivo/experto, cuya responsabilidad es mayor.[5] En la **figura 2** se identifican las diferentes áreas de pericia en seguridad de la información.

Tarea 2: Elaborar estrategias para crear un plan para la adquisición de pericia

El objetivo de esta tarea es desarrollar una estrategia para dominar adecuadamente cada una de las áreas de pericia descritas y superar, de este modo, la brecha que puede impedir que una persona obtenga el puesto deseado por no dominar las competencias fundamentales del cargo. Así, los practicantes podrán concentrarse en las actividades de desarrollo profesional que mejor se ajusten a sus objetivos laborales. Es importante comprender que no hay un único camino para reunir las habilidades, la experiencia y el conocimiento deseados. El desarrollo de un plan personalizado dependerá de la experiencia, capacitación y formación de una persona. Según el nivel jerárquico, la trayectoria profesional, la especialización y el objetivo del cargo de quien elabora el plan, el empleo de distintas estrategias de perfeccionamiento podría proporcionar el medio apropiado para el desarrollo profesional. Todo plan debería:

- Identificar las brechas existentes entre el dominio de competencias fundamentales y los niveles esenciales para ascender un peldaño en la trayectoria profesional de una persona.
- Proporcionar un medio de comunicación para discutir la planificación de la carrera profesional.
- Ofrecer distintas opciones para adquirir las habilidades y experiencia necesarias.

Hay distintos canales para cerrar las brechas identificadas entre el nivel de pericia actual y el deseado. La decisión respecto de la manera en que se cierre esta brecha dependerá de las necesidades de la persona y de otros atributos vinculados a las diversas alternativas de desarrollo presentes, a saber:

- Costos de la opción de desarrollo.
- Profundidad del grado de pericia deseado (familiaridad básica o distintos niveles de experticia).
- Plazos para completar el perfeccionamiento.
- Disponibilidad de reembolsos o ayuda financiera otorgados por el empleador.
- Horario de trabajo.
- Posibilidad de viajar para participar en opciones de desarrollo.

Posiblemente sea necesario combinar varias opciones para obtener un experiencia específica, especialmente en ámbitos sumamente técnicos. Para cerrar la brecha respecto de los niveles de pericia, se pueden emplear las siguientes alternativas:

- **Certificación profesional:** varios estudios han demostrado una tendencia ininterrumpida respecto del pago de salarios más altos para profesionales certificados en seguridad de TI.[6] También se ha demostrado que diversas certificaciones relacionadas con la seguridad redundan en mejores remuneraciones dentro del ámbito de las TI.[7, 8] La certificación aparece con frecuencia como requisito o preferencia en las publicaciones de puestos vacantes para practicantes.[9] No es casual que la certificación, especialmente las designaciones *Certified Information Systems Auditor®* (CISA®) y *Certified Information Systems Security Professional* (CISSP), sea la opción de desarrollo más elegida por los practicantes. Se recomienda a los practicantes realizar una investigación más amplia para explorar otras certificaciones disponibles, además de las opciones conocidas, y evaluar certificaciones más específicas, que se ajusten mejor a su experiencia y objetivos profesionales. Las certificaciones en gobierno, desarrollo seguro, cómputo forense y fraudes son solo

algunas de las alternativas de certificación que se hallan disponibles, y ofrecen a los practicantes la oportunidad de centrarse en trayectorias profesionales específicas. Algunas certificaciones brindan una alternativa de crecimiento al permitir que se profundice en ciertos temas y superar ampliamente el nivel de certificación básico, para que los practicantes puedan distinguirse en un área de seguridad determinado. Otros optan por combinar certificaciones, como las certificaciones de seguridad tradicionales y para proveedores, a fin de distinguirse como "profesionales renacentistas de la seguridad" (*"renaissance security professional"*).[10] Este concepto, acuñado por J.J. Thompson, describe a los profesionales de la información que han desarrollado un conjunto polifacético de habilidades, y que poseen un amplio espectro de conocimientos en materia técnica y de negocios, y una variada experiencia. Diane Morello, vicepresidente de Gartner, los denominó "profesionales híbridos".[11] Según Morello, el profesional híbrido apareció cuando la "intersección de modelos de negocio y TI comenzó a exigir la intervención de personas que tuvieran variada experiencia, versatilidad profesional, conocimiento multidisciplinario y dominio de la tecnología". De acuerdo con el artículo técnico de Forrester, *"The Evolving Security Organization"*, el papel del profesional híbrido permite que los practicantes del campo de la seguridad de la información emerjan de su posición aislada y se conviertan en facilitadores de negocios.[12]

- **Opciones académicas superiores:** en numerosas reuniones de alto nivel de ejecutivos de seguridad de la información (CISO),[13] los participantes debatieron sobre la obtención de títulos académicos de nivel superior como opción de desarrollo profesional. En 2003, la Agencia de Seguridad Nacional (NSA) y el Departamento de Seguridad Nacional (DHS) de los EE. UU. crearon, conjuntamente, un programa para promover el desarrollo de cursos académicos superiores centrados en la seguridad de la información.[14] Durante la década pasada, este tipo de programas prosperó en cantidad y variedad, pero los practicantes deberían examinar los distintos programas académicos en función de sus propias aspiraciones profesionales. Estos programas ofrecen un área de conocimiento específico o proporcionan un enfoque general del campo de estudio. Otra opción consiste en obtener títulos de posgrado en negocios, finanzas o derecho para definir una trayectoria profesional exclusiva. El inconveniente de estas alternativas académicas es que debe invertirse una considerable cantidad de tiempo y dinero para concretarlas. Según una encuesta informal sobre las publicaciones de puestos vacantes, la presentación de un título de posgrado se está convirtiendo en un requisito o preferencia, cada vez más común, de los empleadores para los puestos de mayor responsabilidad.
- **Autoaprendizaje:** numerosas organizaciones profesionales y educativas ofrecen una gran variedad de cursos y materiales de autoaprendizaje. Hay mucho material disponible en línea a un costo razonable, e incluso gratis. Además de los programas basados en la web, los libros siguen siendo una de las opciones más empleadas para obtener conocimientos. El inconveniente de esta opción tal vez resida en el modo de documentar estas alternativas para presentarlas ante los empleadores. El orador Brian Tracy, excelente motivador, recomienda que los profesionales dediquen una hora por día a la lectura.[15]
- **Mejora de las habilidades interpersonales:** las habilidades interpersonales son una de las competencias fundamentales que los asociados de seguridad de la información deben poseer para no perder impulso en sus carreras y mantener su empleo. La habilidades interpersonales complementan las habilidades técnicas y generan credibilidad con los colegas. En las conversaciones sostenidas con numerosos profesionales de la seguridad de la información durante los últimos diez años, un tema recurrente es la necesidad de que los practicantes que han reunido mayor pericia técnica también desarrollen habilidades de comunicación más sólidas, como las requeridas para las operaciones de venta, las negociaciones y las presentaciones. Si bien hay diversos cursos profesionales centrados en estos objetivos, algunos practicantes adquieren estas habilidades saliendo de sus zonas de comodidad para realizar presentaciones en conferencias o dictar cursos (a nivel interno o externo). Otras opciones incluyen la capacitación en ventas y los grupos de oratoria.
- **Experiencia práctica y designación de mentores:** no todas las habilidades se obtienen a través de los libros o las clases; a veces, no hay nada que pueda sustituir a la experiencia en "el mundo real". Una de las mejores estrategias para obtener la pericia necesaria es buscar un mentor o experto en un tema para observar y aprender primero, y para trabajar después junto a esas personas, asumiendo poco a poco un mayor volumen de las tareas requeridas para un trabajo en particular. Un buen ejemplo de esta práctica es el proceso de aprendizaje para la realización de evaluaciones de riesgo de seguridad de los proveedores. El aprendiz podría comenzar simplemente acompañando a un auditor o asesor de riesgos especializado. Más adelante podría ir asumiendo distintas tareas hasta que esté listo para "volar solo", mientras el mentor evalúa su competencia profesional. Esta estrategia también es aplicable a los profesionales de seguridad de la información que desean "refrescar" sus habilidades o explorar nuevas alternativas para realizar una tarea determinada. Otra excelente opción es asumir la función de mentor de otro practicante.

PASO 4: REALIZAR VERIFICACIONES REGULARES DE STATUS

Evaluar el avance resulta indispensable. Es muy fácil salirse del rumbo o perder impulso cuando el trabajo nos conduce en direcciones no deseadas. Existen algunas señales de

advertencia de estancamiento en la carrera profesional, entre ellas:

- No profundizar en el desarrollo de habilidades y capacidades.
- No ser elegido para integrar nuevos equipos o participar en nuevos proyectos, salvo raras excepciones.
- Perder el entusiasmo por el trabajo.
- No realizar ninguna actividad de desarrollo profesional durante más de un año.
- Calcular los días que faltan para jubilarse.

Si bien la recesión económica y la consiguiente reducción del presupuesto asignado a capacitación impactan negativamente en el desarrollo profesional de quienes disponen de opciones más limitadas para su desarrollo profesional, resulta esencial, incluso en mercados laborales difíciles, seguir teniendo relevancia y permanecer actualizados en la especialidad elegida, aunque esto solo pueda realizarse leyendo libros o asistiendo a cursos de capacitación de bajo costo. Regularmente (cada seis meses o cada año, por ejemplo), se debería revisar el progreso obtenido en relación con lo planeado y realizar los ajustes necesarios. Los planes de desarrollo de competencias fundamentales siempre deben ser documentos vitales, en constante evolución.

CONCLUSIÓN

¿Qué se hace con el colega que posee habilidades limitadas a pesar de sus más de 20 años de experiencia? Algunos podrían decir que "tiene un año de experiencia repetido 20 veces".[16]

Las competencias fundamentales no son estáticas, especialmente en los campos de índole técnico, como el de la seguridad de la información. Nunca debemos dejar de aprender. En su libro —hoy considerado un clásico— *Los siete hábitos de las personas altamente eficaces*, Stephen Covey describe un hábito que denomina "afilar la sierra", que insta a aprender algo nuevo y adquirir distintas experiencias continuamente.[17] Esto es similar a la filosofía Kaizen ("mejora") japonesa, que describe mejoras o cambios superadores, centrándose en la mejora continua de los procesos. Alguna vez, Stephen Covey recomendó "comenzar con el objetivo en mente".[18] Este concepto sigue siendo válido. Los practicantes y profesionales de la seguridad de la información siempre tienen la posibilidad de modificar el destino de sus carreras, y el modelo de competencias fundamentales que aquí se describe puede servir de ayuda para alterar el rumbo, en dirección a esa meta.

> "Nunca debemos dejar de aprender."

NOTAS FINALES

1 Traducción de las definiciones de los términos *'practitioner'* y *'professional'*, tomadas de Merriam-Webster Dictionary, *www.merriam-webster.com*

2 Newman, Rick; *Rebounders: How Winners Pivot From Setback to Success*, 2012

3 BrainyQuote, *www.brainyquote.com/quotes/quotes/b/benjamindi130016.html*. Benjamin Disraeli (1804-81) fue un estadista británico.

4 Estos niveles están basados en la encuesta del autor sobre publicaciones de puestos vacantes en el área de seguridad de la información.

5 Este modelo fue adaptado de *ARMA Records and Information Management Core Competencies* (2008), al igual que la encuesta del autor sobre las publicaciones de puestos vacantes en el área de seguridad de la información.

6 Vijayan, Jaikumar; "Salary Premiums for Security Certifications Increasing, Study Shows", *ComputerWorld*, 9 de julio de 2007, *www.computerworld.com/s/article/9026624/Salary_premiums_for_security_certifications_increasing_study_shows*

7 Muller, Randy; "15 Top Paying IT Certifications for 2012", Global Knowledge, enero de 2012, *www.globalknowledge.ca/articles/generic.asp?pageid=3159&country=Canada*

8 Gupta, Upasana; "Top 5 Certifications for 2012", GovInfoSecurity.com, 2 de diciembre de 2011, *www.govinfosecurity.com/top-5-certifications-for-2012-a-4291/op-1*

9 Basado en la propia encuesta del autor sobre publicaciones de puestos vacantes en los últimos años

10 Bedell, Crystal; "The Renaissance Security Professional: Skills for the 21st Century", (ISC)²

11 Gartner, "Gartner Warns of a Looming IT Talent Shortage", 2008, *www.gartner.com/it/page.jsp?id=600009*

12 Kark, Khalid; Bill Nagel; *The Evolving Security Organization*, Forrester, 26 de julio de 2007

13 El autor ha asistido a más de 50 eventos relacionados con la seguridad de la información, incluidas cinco cumbres CISO, donde se debatió sobre desarrollo profesional y formación académica superior.

14 National Security Agency, "National Centers of Academic Excellence", *www.nsa.gov/ia/academic_outreach/nat_cae/index.shtml*

15 Tracy, Brian; "One Hour Makes All the Difference", *www.briantracy.com/blog/personal-success/one-hour-makes-all-the-difference/*

16 Esta cita pertenece al hermano del autor. El autor encontró varias referencias a citas similares, incluso en *Geeks, Geezers, and Googlization: How to Manage the Unprecedented Convergence of the Wired, the Tired, and Technology in the Workplace*, libro escrito por Ira S. Wolfe y publicado recientemente.

17 Covey, Stephen; *The Seven Habits of Highly Effective People*, Free Press, 1989

18 *Op. cit.*, Covey