Maestría en Administración de Empresas Énfasis Gerencia de Operaciones

Investigación Empresarial Aplicada

La competitividad laboral en Costa Rica: el caso de la formación de los profesionales en seguridad informática

Gustavo Santana Baldares
ULACIT 2015

TABLA DE CONTENIDOS

Resumen ejecutivo 2
Palabras claves 3
Abstract 3
Key Works 4
Tema: La competitividad laboral en Costa Rica: el caso de la formación de los profesionales en seguridad informática 4
Capítulo I. Antecedentes e importancia del problema 5
Antecedentes 5
Justificación 5
Problema de investigación 6
Objetivos 7
Objetivo general 7
Objetivos específicos 7
Forma de alcanzar los objetivos 7
Capítulo II. Revisión bibliográfica 8
Capítulo III. Metodología de la investigación 12
Capítulo IV. Análisis y discusión de resultados 14
Referencias 22
Anexos 23
Instrumento de la investigación 23

Resumen ejecutivo

La presente investigación se enmarca dentro de los objetivos institucionales de ULACIT, para enfocar los proyectos de investigación en torno al tema global de la competitividad laboral en el país. En este caso en particular, el objeto de estudio se delimitó al área de la seguridad informática, debido a la experiencia personal del investigador con el tema y a la preocupación que existe a nivel nacional con respecto a la mano de obra que se requiere en los distintos campos o sectores productivos, para asegurar el desarrollo del país y la empleabilidad de los trabajadores.

Por la naturaleza de la investigación, el método seleccionado es cualitativo, ya que permite una mayor amplitud en el planteamiento del problema y mayor flexibilidad para la obtención de los datos que se recopilaron por medio de la aplicación de entrevistas semiestructuradas. La investigación también es descriptiva y exploratoria, ya que procura describir situaciones y eventos de temas poco explorados o novedosos en el país.

El estudio evidenció que en Costa Rica es creciente la necesidad de contar en las empresas con personal especializado en seguridad informática. No obstante, no existe claridad acerca del perfil profesional requerido ni sobre las competencias deseables en el profesional, aparte de que existe un total desconocimiento de las implicaciones de los grados de nivel técnico, pese a la aparente necesidad que tiene el país de contar con profesionales calificados.

Se concluye que en el área de seguridad se están dando los primeros pasos y que para ser competitivos, se requiere que las empresas cuenten con profesionales con formación completa o técnica, ya que esto dependerá de las necesidades, condiciones financieras y características de cada entidad; de sus perspectivas de crecimiento o transformación; o del cumplimiento obligatorio de disposiciones normativas sobre seguridad, como en el caso de las empresas transnacionales.

Finalmente, las recomendaciones apuntan a la necesidad de contar con especialización en una serie de temas específicos que se indican de manera detallada y que responden al estudio de los referentes internacionales más avanzados en el área.

Palabras claves

Seguridad informática/ empleabilidad/ competitividad/ formación técnica/ tecnología de información.

Abstract

This research is part of the institutional objectives of ULACIT to focus research projects on global issue of labor competitiveness in the country. In this particular case, the object of study was delimited in the area of Information Technology Security because of the personal experience of the researcher with the issue and concern that exists at national level regarding the labor that is required in various fields or productive sectors in order to ensure the country's development and employability of workers.

By the nature of the research, qualitative method is selected because it allows greater latitude in the problem statement and greater flexibility for obtaining the data collected through the application of semi-structured interviews. The research is descriptive and exploratory as it seeks to describe situations and events unexplored or novel issues in the country.

The study showed that in Costa Rica is increasing the need for companies specialized in computer security personnel. However, there is no clarity about the professional profile required or on the desirable skills in the professional apart from that there is total ignorance about the implications of degrees of technical level despite the apparent need for the country to have professionals with this degree.

It is concluded that in the area of security are in the early stages and that to be competitive requires that companies are experts with full or technical training as this will depend on the needs, financial conditions and characteristics of each entity and its growth prospects or processing or mandatory compliance security provisions such as transnational corporations. Finally the recommendations point to the need for expertise in a number of specific issues that are targeted in detail and respond to the study of the most advanced international benchmark in the area.

Key Works

Information security/employability/competitiveness/technical training/information technology.

Tema: La competitividad laboral en Costa Rica: el caso de la formación de los profesionales en seguridad informática

Capítulo I. Antecedentes e importancia del problema

Antecedentes

En Costa Rica existen estudios promovidos por entidades gubernamentales; por alianzas privadas como CINDE, Amcham o CAMTIC; o por entidades sin fines de lucro como la OIT, que han hecho referencia a la existencia de carreras o profesiones saturadas en el mercado y han señalado las profesiones que en un futuro cercano podrían ser consideradas de alta demanda laboral.

Ante la considerada proliferación de profesionales y saturación de algunas áreas, es frecuente el llamado a la formación de técnicos en áreas ingenieriles, pero sin que exista una adecuada fundamentación o evidencia en el caso concreto de la seguridad informática como área dentro de las tecnologías de la información (TI).

Justificación

Uno de los grandes retos que Costa Rica debe asumir con mayor responsabilidad es asegurar la competitividad de su fuerza laboral, de manera que pueda mantener la empleabilidad de sus ciudadanos en condiciones de seguridad social; y el cumplimiento de las condiciones legales mínimas que establece la legislación nacional, y los cuerpos normativos internacionales que regulan el trabajo como un derecho humano fundamental.

Este reto implica una serie de consideraciones de distinta naturaleza, ya que entre otros aspectos, la competitividad del mercado laboral tiene que ver con temas como generación de empleo; dinamización de la economía nacional; atracción de inversiones; fomento del emprendimiento individual; preparación técnica y académica de los trabajadores; y creación de una oferta educativa que satisfaga las necesidades presentes y futuras de los empleadores, asegurándoles que podrán contar con los trabajadores especializados que requieran, de acuerdo con las necesidades de cada tipo particular de industria.

Dentro de este contexto, un tema de frecuente discusión es la aparente y urgente necesidad de orientar la formación del trabajador costarricense hacia el sector técnico, considerando

entre otros aspectos, la saturación de algunas disciplinas o requerimientos especializados que la mano de obra actual no logra satisfacer.

El llamado a la formación técnica que se realiza a nivel nacional no debe ser considerado a la ligera y, por el contrario, es necesario contar con insumos para que tanto los centros educativos como los mismos estudiantes tengan información suficiente y clara para tomar decisiones de definición vocacional, conociendo las expectativas reales que les ofrece un determinado programa a corto plazo cuando se incorporen al mercado laboral.

En este sentido, este llamado a la formación técnica requiere considerar aspectos tales como qué se debe entender por ese grado académico, cuál es la demanda real actual y a corto plazo en los distintos sectores de profesionales técnicos, cuáles son las competencias que un empleador espera de un técnico, cuáles deberían ser los factores de diferenciación entre un profesional técnico y un bachiller en el mismo campo y cuáles son las diferencias salariales, entre otros.

Problema de investigación

Para efectos de la presente investigación, con la finalidad de delimitar el tema y de analizarlo a la luz de un área de reciente demanda en el país como parte de las funciones propias de los departamentos de Tecnología de Información en las empresas y organizaciones, se propone como problema de investigación el análisis de la realidad nacional sobre la formación, empleabilidad actual y futura, y competencias requeridas en el área de seguridad informática.

El problema se manifiesta por medio de la siguiente pregunta de investigación: ¿Cuál es la necesidad real de profesionales a nivel técnico en seguridad informática en Costa Rica, para cubrir las necesidades de dicho sector, y cuál es el perfil profesional requerido?

Objetivos

Para responder con propiedad la pregunta de investigación propuesta, se plantean los siguientes objetivos.

Objetivo general

- Diseñar una propuesta para la formación de personal con nivel técnico especializado en seguridad informática, de acuerdo con las necesidades del sector productivo, a fin de satisfacerla con la oferta actual de trabajadores y asegurar así la competitividad del sector.

Objetivos específicos

- Identificar la definición operacional que se tiene del grado "técnico" en el sector de tecnologías de información.

- Determinar la necesidad de personal especializado técnico en seguridad informática en el sector de tecnologías de información.

- Diferenciar las competencias y el perfil profesional en seguridad informática que se requieren para un profesional con un grado técnico.

Forma de alcanzar los objetivos

Con la finalidad de alcanzar los objetivos propuestos en la presente investigación, se construyó un marco teórico que permitió identificar ─a partir de referentes internacionales y nacionales─ la pertinencia e impacto de los profesionales en seguridad informática dentro de la estructura de las empresas e instituciones. Este apartado analiza, además, los retos por los que atraviesan los sectores, con la finalidad de identificar las necesidades de capacitación a fin de diseñar en el país una oferta académica que asegure la competitividad y la empleabilidad del personal.

Para conocer la percepción de los profesionales que trabajan en el área en términos de la necesidad de oferta laboral técnica, las oportunidades de mejora que consideran que se deben incorporar al perfil y las competencias que identifican en el personal deseable, se diseñó un instrumento de evaluación (encuesta semiestructurada) que se aplicará al menos a 10 personas involucradas en el tema. La información recolectada se analizó y sistematizó, para que sirviera como insumo válido para la presente investigación.

Capítulo II. Revisión bibliográfica

La tendencia empresarial moderna apunta a destacar la relevancia estratégica de los departamentos de tecnología de información de manera que no es extraño identificar que los directores de esta área reportan directamente a los consejos directivos o pertenecen a estos órganos. Esto se debe mayoritariamente al hecho de que las soluciones y propuestas tecnológicas de las empresas son indispensables para su desarrollo y expansión, pues contribuyen con el objetivo de mejorar globalmente el negocio, independientemente del sector en que opere.

En este sentido, Díaz (2012) señala que "hoy más que nunca las estrategias de TI trabajan en función de los objetivos institucionales de la empresa y se han convertido en un elemento fundamental en la gestión de los líderes empresariales" (p.1).

De acuerdo con Díaz (2012), es necesario reconocer que las tecnologías de la información (TI) son vitales en todo tipo de organizaciones, entre otras razones por la capacidad de almacenar, procesar y distribuir datos por medio de las computadoras, lo que las convierte en herramientas esenciales en la gestión; por lo tanto, la estrategia de los departamentos debe estar alineada a los objetivos organizacionales, a fin de velar por una adecuada asignación y uso de los recursos.

Dentro de este contexto que rodea la realidad de las áreas de TI, es necesario considerar que como parte de la administración y minimización de riesgos y las consideraciones acerca de cómo disminuir la vulnerabilidad de las empresas, ha sido necesario rediseñar las estructuras, para incluir modelos de seguridad que permitan cubrir no solo los riesgos tradicionales, sino también los que se puedan ir generando sobre la marcha del quehacer institucional.

Actualmente se considera el tema del riesgo como un área funcional y especial de las organizaciones, dado que existen pérdidas que pueden ser desde subsanables, de considerable magnitud o capaces de poner en riesgo las operaciones e incluso la supervivencia de las empresas. Por esta razón es que es deseable que a nivel directivo en las empresas y organizaciones, se valore si se cuenta con políticas, manuales o procedimientos que al menos cubran la protección de datos, políticas, normas y directrices; y que se identifique la importancia de la seguridad en el ciclo de vida de los sistemas de información, de manera que se gestione un plan de seguridad con los recursos humanos y materiales necesarios.

De acuerdo con Business Alliance for Secure Commerce-Costa Rica (2008), entre los riesgos típicos a los que resultan principalmente vulnerables las organizaciones, se encuentran ─sin orden de relevancia─ los siguientes:

- Influencia de personas internas o ajenas a la organización.
- Intervenciones por hecho fortuito o causa mayor ocasionadas incluso por la naturaleza.
- Calidad deficiente o poco confiable en los servicios o suministros.
- Abuso en el manejo de los recursos o sistemas informáticos.
- Intervención dolosa o de mala fe por parte de terceros que causan daños o deterioros en equipos o en actividades.
- Descuido en el manejo y resguardo de la información por parte de los usuarios.

Por lo anterior, dada la relevancia de la seguridad informática en las organizaciones, es cada vez más frecuente encontrar que las áreas de TI estén estructuradas en los siguientes sectores: infraestructura y telecomunicaciones, desarrollo y administración de sistemas, servicios de soporte, y seguridad y cumplimento. Para cada área o departamento es necesario contar con personal con el perfil profesional especializado, dado que no es viable presumir que un graduado a nivel de bachillerato posea las competencias para desempeñarse de forma competitiva en todas las ramas.

Pese a que la tendencia empresarial orientada hacia la contratación de personal especializado en seguridad informática parece estar poco documentada en Costa Rica, en países como Estados Unidos sí existen referencias que permiten afirmar que la demanda no logra cubrirse con la oferta disponible. Por ejemplo, en un informe de Burning Glass Technologies, se plantea que la demanda de profesionales de ciberseguridad creció 3,5 veces más rápidamente que otros trabajos de TI, y 12 veces más rápidamente que todos los otros trabajo (Tirado, 2000).

Este mismo estudio señala que los puestos más demandados por las empresas fueron precisamente el de ingenieros de seguridad de la información y analistas de seguridad, y que estos fueron requeridos en sectores ubicados en servicios financieros, comercio, salud y servicios profesionales. La falta de profesionales especializados ha incidido en dos aspectos importantes para el mercado laboral y su competitividad: por una parte, las empresas demoran más tiempo del previsto para realizar las contrataciones de personal capacitado; y, y por otra, la escasez ha ocasionado mejoras salariales para los profesionales en seguridad.

De acuerdo con la Revista IT Now (2015), la tendencia norteamericana ha sido que en algunas empresas se ha solicitado a los empleados contar con certificaciones en seguridad, para identificar a los funcionarios aptos para los puestos, pero además empiezan a identificarse algunos rasgos importantes para definir el perfil profesional, ya que la preferencia de los empleadores apunta a trabajadores certificados pero con experiencia y

familiarizados con temas como políticas, procedimientos y gobernanza de seguridad en redes.

En este mismo orden de ideas, un estudio realizado por CompTIA señala que la seguridad informática es la prioridad para las tres cuartas partes de los directores de contratación TI entrevistados, con lo cual se evidencia el crecimiento de la demanda de profesionales expertos en esta disciplina y la necesidad de contar con recurso humano con conocimientos en áreas como redes, *wireless*, aplicaciones y sistemas operativos, *firewalls*, filtración de datos o cumplimiento normativo (Network world, 2008).

De acuerdo con Pinto (2009), es necesario contar con una política educativa que satisfaga la creciente demanda de recursos humanos calificados en cuanto a cantidad y calidad, y si bien es cierto que las universidades y sus graduados son importantes, se debe valorar la formación técnica y parauniversitaria. No obstante, "si bien, se debe apoyar la educación técnica, se debe tener cuidado de no transformar este sector en una industria de servicios de poco valor agregado, intensiva en empleo" (Pinto, 2009, p. 64).

Asimismo, como parte de la estrategia que se recomienda, se indican tareas prioritarias tales como actualizar los conocimientos, habilidades y destrezas de los graduados; revisar la idoneidad de los programas actuales en computación e informática; y crear nuevos programas. Es decir, todas estas son estrategias relacionadas con aspectos de índole académico o que se deben responder desde la dimensión educativa, por lo que claramente hay una necesidad de formar profesionales con rango de "nivel técnico" como parte de la propuesta.

Por otra parte, propiamente en términos de apoyo a la competitividad de las tecnologías de la información y la comunicación (TIC), Pinto (2009) propone objetivos en el orden del fortalecimiento de la educación pública y privada, fortalecimiento de la educación técnica y parauniversitaria, aumentar el número de graduados del sector y promover grados alternos al bachillerato y salidas laterales a este mismo grado.

Nótese que este informe al que se ha hecho referencia aborda de manera clara la problemática nacional en términos de TIC en general, sin realizar mayor énfasis en cada área (al menos la seguridad informática no se analiza de manera particular), pero sí es un valioso referente contextualizado a la realidad nacional y que hace alusión al presente problema de investigación, en relación con el perfil de los graduados a nivel de especializaciones técnicas.

De acuerdo con lo anterior, la necesidad de responder con personal calificado a los requerimientos del sector tecnológico es un reto que Costa Rica debe atender de manera ineludible, sin dejar de lado una de las áreas de mayor demanda e impacto como lo es la de la seguridad informática. El reto de la presente investigación radica en responder a la interrogante planteada acerca de la necesidad real de este tipo de profesionales con nivel de formación técnica, y determinar los rasgos del perfil ocupacional necesario para su inserción exitosa en el mercado laboral.

En lo que respecta a la operacionalización del grado académico de "técnico", de acuerdo con el Convenio para Crear la Nomenclatura de Grados y Títulos de la Educación Superior Universitaria Estatal, vigente desde el 2004, no existe este grado en ninguna de las distintas opciones disponibles en el país a nivel universitario.

Este Convenio es el documento oficial que se utiliza en el país para la creación de carreras o programas oficiales, e incluye a nivel de pregrado a los diplomados y los profesorados; en los niveles de grado, a los bachilleratos y licenciaturas; y en posgrados, a las maestrías y doctorados.

Capítulo III. Metodología de la investigación

El problema de investigación se plantea a partir de la interrogante de cuál es la necesidad de profesionales a nivel técnico en seguridad informática en Costa Rica, y cuál es el perfil profesional para satisfacer esa demanda.

A partir de este problema de investigación, para efectos metodológicos, se seleccionó el enfoque cualitativo, que se caracteriza por admitir una mayor amplitud en el planteamiento del problema que surge luego de un proceso inductivo por medio del cual se explora y se proponen teorías que evolucionan hasta una conclusión general. La investigación es descriptiva ─modalidad que procura describir situaciones y eventos con precisión, requiriéndose por parte del investigador conocimientos previos sobre el objeto de investigación─ y también exploratoria, ya que se pretende ofrecer una visión general del tema, ya que ha sido poco explorado y es novedoso a nivel nacional (Barrantes, 2009).

Este modelo cualitativo se caracteriza por tratar de situar la investigación en relación con lo que el investigador conoce del tema, sin dejar de lado la revisión de la literatura y el objetivo final, que es demostrar una teoría y que los resultados obtenidos se extrapolen a otros fenómenos u objetos de estudio.

La población deseable para obtener los datos son profesionales de TI, especialistas en reclutamiento y selección de personal y en seguridad y protección de datos informáticos, y profesionales afines que laboran en el campo académico por su permanente vinculación con el problema investigado.

Para efectos metodológicos, se seleccionó como instrumento para colectar los datos la entrevista semiestructurada, la cual se aplicó a una muestra de 10 personas, pertenecientes a la población indicada, procurando obtener información que permitiera analizar las variables de la investigación a partir de su experiencia laboral.

En opinión de Hernández, Fernández y Baptista (2010), la entrevista en la investigación cualitativa se realiza a partir de una guía, pero quien entrevista tiene la posibilidad de introducir nuevas preguntas o enfoques para alcanzar mayor profundidad y mejores resultados de la información.

Previo a la aplicación de las entrevistas, se diseñó una matriz que sirvió de apoyo durante el proceso, ya que le facilitó al investigador incorporar por escrito y de forma simultánea a la entrevista, los elementos claves de las respuestas, de manera que se favoreciera la síntesis posterior de los hallazgos más importantes.

La recolección de los datos correspondió a este tipo de enfoque, caracterizado porque "los datos que interesan son conceptos, percepciones, imágenes mentales, creencias, emociones, interacciones, pensamientos, experiencias, procesos y vivencias que se recolectan con la finalidad de analizarlos y comprenderlos, y así responder a las preguntas de investigación y generar conocimiento" (Hernández et al., 2010, p.277).

Finalmente, concluida la aplicación de las entrevistas, se revisó y ajustó la matriz diseñada, con la finalidad de asegurar la incorporación de toda la información relevante, e identificar elementos comunes y puntos de diferencia entre los relatos de los entrevistados, con la finalidad de tener claridad sobre el ejercicio de recolección de datos y los resultados obtenidos.

Capítulo IV. Análisis y discusión de resultados

En el presente capítulo se retoma el problema de investigación y sus objetivos, para posteriormente exponer los datos relevantes de la investigación o los principales hallazgos como resultado de la aplicación de las entrevistas.

A partir de la realización de las entrevistas, se identificaron hallazgos importantes, que permiten ser seleccionados como las variables que mayor relevancia tienen para efectos de la investigación.

En primer lugar, los entrevistados coinciden en señalar que cada vez más es frecuente que en sus empresas se discuta sobre la necesidad de contar con personal de planta especializado en seguridad informática, aunque no en todas estas empresas se cuente actualmente con ese funcionario, ya sea por razones presupuestarias o por no estar tan presente la necesidad real pero si la proyección a corto plazo.

Una excepción a esta afirmación se da en el caso de empresas trasnacionales, en las que debido a la obligatoriedad de cumplir con regulaciones para poder operar tanto en Estados Unidos como en Europa, se hace imprescindible la adopción de estándares como Sarvanes –OXlEY e ISO 27.001, que imponen controles para evitar fraudes y riesgos de bancarrota por alteración de información sensible. Estos controles son obligatorios en el caso de

empresas que cotizan en la Bolsa de Valores de EE. UU., en cuyo caso los estándares de seguridad para las empresas se incrementan de manera exponencial.

Otro hallazgo interesante que se desprende de las entrevistas es que en algunas empresas, por razones financieras, no es viable contar con personal de planta en el área de seguridad informática, pero al menos se refuerza la cobertura con la contratación bajo la modalidad de *outsourcing*, con lo cual se confirma que en diversas modalidades, las empresas reconocen la importancia y relevancia reciente de estos especialistas.

Reconocida la necesidad de la plaza o puesto, los entrevistados coinciden en señalar que las contrataciones no resultan sencillas, dada la escasa demanda de personal especializado. En este punto en particular, los entrevistados del área de recursos humanos señalan las siguientes dificultades:

- No existe en el país una alta demanda de personal graduado con un énfasis en el área.
- La mayor parte de la oferta de personal graduado en ingeniería informática o sistemas en el país, no ha recibido como parte de su formación general cursos o contenidos suficientes para considerarlos especialistas.
- Algunos empresarios o reclutadores no se sienten especialmente inclinados por contar con personal graduado, sino más bien por incorporar en sus empresas a personal con certificaciones en el tema o bien ir capacitando progresivamente a su personal vigente.

Respecto a la formación técnica o especializada que se requiere, los entrevistados coinciden en señalar que esto dependerá en gran medida del tamaño de la empresa y de los compromisos que tenga, de acuerdo con las características antes detalladas para empresas transnacionales. Indican que en esto incide el rumbo del país y de su capacidad para atraer nueva inversión extranjera y retener la ya existente, dado que en este tipo de empresas los requerimientos suelen ser más complejos, rigurosos y obligatorios.

En términos generales, se afirma que lo relevante no es el grado académico del especialista, sino lo que este es capaz de hacer en la empresa o en la organización; la

capacidad para aprender, para estudiar e investigar sobre las mejores prácticas en el sector de acuerdo con cada tipo de industria; y su interés por la formación o aprendizaje continuo.

Si se trata de una contratación de un profesional con un grado "técnico", los entrevistados (excepto los académicos), reconocen no tener mayor criterio para diferenciar o explicar qué se entiende por este grado, aunque sí son claros en explicar que un "técnico" no es lo mismo que un "ingeniero", y con base en ese aspecto, es claro que la diferencia salarial sería significativa. Además, reconocen que de acuerdo con los mecanismos de compensación y beneficios con los que se trabaja en sus empresas, las posibilidades de ascenso para este personal es reducido, ya que precisamente el logro o adquisición de grados académicos es esencial para escalar posiciones.

En términos generales, todos los grupos consultados consideran que un técnico no es necesariamente un profesional, sino precisamente "solo un técnico", que a lo suma cuenta con estudios de al menos un año y al que no se le podrían asignar puestos de jefatura o de dirección de proyectos bajo su entera responsabilidad.

En este último sentido coinciden los entrevistados del área de reclutamiento o recursos humanos, aunque señalan que usualmente los grados "técnicos" son un escalón para mejorar el reclutamiento y son una excelente propuesta académica para motivar al personal (sobre todo al más joven), para continuar con su formación académica al no conformarse o limitarse con ese grado.

En el caso de los entrevistados que están vinculados con el sector académico y docente, parece estar muy clara la necesidad de diseñar programas que aseguren la formación de la oferta que el país necesita; sin embargo, reconocen dificultades para el diseño de estos programas, dada la poca experiencia que existe en el país y que redunda en escasez de personal especializado que aporte desde el diseño curricular y sobre todo en la docencia.

Este sector reconoce que ciertamente a nivel nacional se ha recibido una significativa presión para promover la formación de "oferta profesional técnica", pero reconocen no tener claridad acerca de las expectativas de conocimientos o de perfil profesional que se espera en cada área. Desconocen las expectativas de cada una de las áreas de los sectores productivos y, aun más, admiten sentir preocupación por las posibilidades reales de

contratación de esa mano de obra y sobre la disponibilidad de remuneración que las empresas estén dispuestas a ofrecer, ya que al final este es uno de los criterios de mayor influencia para decidirse o no por un determinado programa.

Finalmente, acerca de la consulta planteada sobre si el personal con el que laboran cuentan con las competencias necesarias que requieren las empresas y organizaciones, la mayoría de los entrevistados reconoce que por lo novedoso y cambiante del mundo de la seguridad informática, ellos mismos carecen de grandes conocimientos que les permitan evaluar y direccionar a su personal.

Reconocen que sobre la marcha, ellos mismos han debido aprender e incluso en algunos casos optar por capacitaciones formales o por autoaprendizaje. En las empresas de mayor tamaño o en las de carácter transnacional, lo normal ha sido la inversión en capacitación dentro y fuera del país, y la adopción de normas y políticas de carácter internacional o corporativo para ir implementando el área dentro de sus departamentos.

En algunos casos, los entrevistados afirman conocer casos referidos por terceras personas en empresas nacionales, en las que han atravesado dificultades por no contar con especialistas en seguridad informática o al menos con empleados certificados en algunas de las principales capacitaciones o entrenamientos existentes en el mercado. No siempre en estos casos la experiencia desafortunada llevó a un proceso de aprendizaje que culminara con la contratación de especialistas y menos con la creación de un área dedicada exclusivamente al tema.

En términos generales, los entrevistados coinciden en la necesidad de disponer de personal especializado en seguridad informática. Prevén, a corto plazo, un incremento en las contrataciones bajo distintas modalidades de personal entrenado o certificado; reconocen el impacto positivo de las políticas en las empresas y organizaciones, de modo que estarían dispuestos a su adopción e implementación aun cuando no fuera obligatorio realizarlo; y admiten la necesidad de capacitación a título personal y para sus colaboradores, optando por entrenamiento dentro y fuera del país.

En general, no se sienten cómodos opinando sobre los perfiles académicos y profesionales de esta oferta laboral, y suelen por lo general privilegiar la especialización de los

profesionales ya existentes en sus empresas, antes que la contratación de especialistas con carreras cortas. Respecto a la necesidad de mano de obra con un grado técnico, no se atreven a opinar con propiedad, reconocen no tener muy claro el significado y cobertura de este grado académico, y prefieren inclinarse por entrenar al personal actual.

Capítulo V. Conclusiones y recomendaciones

De conformidad con el problema planteado en la presente investigación, se propuso determinar la necesidad real de profesionales en seguridad informática en Costa Rica, y el perfil profesional requerido a nivel técnico para atender adecuadamente las necesidades del sector productivo, a fin de asegurar la competitividad del sector laboral.

Considerando la literatura consultada, los resultados de las entrevistas y la experiencia, a nivel de conclusiones de la presente investigación, se puede afirmar que la tecnología de información tiene en Costa Rica áreas muy consolidadas como lo son el análisis y desarrollo de sistemas, infraestructura y telecomunicaciones, y servicios de soporte.

Por el contrario, en el área de seguridad y cumplimiento, apenas se están dando los primeros pasos en el país y para el éxito en su implementación se requiere que las empresas cuenten con profesionales tanto con formación completa como técnica, ya que esto dependerá de las necesidades, condiciones financieras y características de cada empresa y sus perspectivas de crecimiento o transformación.

La aseveración de la necesidad de formación de especialistas con grado técnico en el país no queda confirmada en el caso particular de la seguridad informática, con base en la presente investigación. Entre otras razones, esto se da por privilegiarse al personal con grado académico de bachillerato (ingeniero) o por un reconocido desconocimiento acerca de los alcances de una formación técnica. Pese a esto, sí es clara la necesidad de capacitación continua o permanente del personal, en los temas que las empresas consideran de mayor relevancia, de acuerdo con sus propias experiencias en el tema.

A continuación se exponen de forma sintética propuestas viables para responder a los principales hallazgos identificados durante el proceso de investigación, desde el punto de vista de diseño curricular, de modo que se establece que es deseable que los profesionales entrenados en esta materia cuenten con capacitación suficiente que les permita desempeñarse como mínimo en los siguientes temas:

- Seguridad de la información y gestión de riesgos.
- Sistemas y metodología de control de acceso.
- Criptografía.
- Seguridad física.
- Arquitectura y diseño de seguridad.
- Legislación, regulaciones, cumplimiento de las mismas e investigación.
- Seguridad de red y telecomunicaciones.
- Planes de continuidad del negocio y de recuperación frente a desastres.
- Seguridad de aplicaciones.
- Seguridad de operaciones.

Las recomendaciones anteriores deben ser consideradas por los centros educativos desde una doble perspectiva, de modo que sirvan de base para el diseño de un programa corto (tal y como se conciben inicialmente los programas técnicos), o bien como materias de énfasis o electivas a nivel de grado o posgrado.

Si se valorara la opción de programas cortos o técnicos, considerando que estos podrían acercarse a los pregrados, el diseño curricular debería partir de los mínimos establecidos para este nivel. En este caso, se debe considerar que un diplomado se considera una carrera corta y debe tener como mínimo 60 y como máximo 90 créditos, con un mínimo de 4 ciclos lectivos y un máximo de 6 ciclos de 15 semanas cada uno y requiriendo de forma obligatoria contar con el bachillerato en educación media. A partir de esta definición operacional del diplomado, pareciera que el grado técnico puede diseñarse de una manera más flexible, dado que no existe un referente técnico para su regulación siendo lo común en la práctica nacional diseños que incluyen entre 8 y 10 materias impartidas en un máximo de 9 meses.

Por otra parte, dada la globalización de la seguridad informática y la interconexión entre empresas, es necesario considerar tanto para nuevos especialistas como para los profesionales actuales, las múltiples opciones que ofrecen entes certificadores para personal de seguridad que les permiten ir escalando y perfeccionándose dentro del área. Dentro de estas opciones, como indispensables se cuenta con:

ISC2:

- CISSP (Certified Information Systems Security Professional) una de las más reconocidas certificaciones a nivel mundial en seguridad informática.

ISACA:

- CISM (Certified Information Security Management) define los principales estándares de competencias y desarrollo profesionales que un director de seguridad de la información debe poseer, competencias que son necesarias para dirigir, diseñar, revisar y asesorar un programa de seguridad de la información.

EC-Council:

Es una de los entes con mayor cantidad de certificaciones y especializaciones dentro de la seguridad informática, entre ellas las siguientes:

- Certified EC-Council Instructor (CEI)
- Certified Ethical Hacker (CEH)
- Certified Network Defense Architect (CNDA)
- Certified Secure Computer User (CSCU)[4]
- Computer Hacking Forensic Investigator (CHFI)
- EC-Council Certified Chief Information Security Officer (CCISO)
- EC-Council Certified Computer Investigator (ECCI)
- EC-Council Certified Encryption Specialist (ECES)
- EC-Council Certified Incident Handler (ECIH)
- EC-Council Certified Secure Programmer-Java (ECSP)
- EC-Council Certified Security Analyst (ECSA)

- EC-Council Certified VOIP Professional (ECVP)
- EC-Council Network Security Administrator (ENSA)
- Licensed Penetration Tester (LPT)

Referencias

Barrantes, R. (2009). *Investigación: un camino al conocimiento. Un enfoque cualitativo y cuantitativo*. San José, Costa Rica: EUNED.

Business Alliance for Secure Commerce-Costa Rica. (2008). *Riesgos Informáticos*. Recuperado de www.basc-costarica.com

Díaz, A. (2012). *La importancia de las estrategias de TI en las empresas*. Recuperado de http://www.esan.edu.pe/conexion/actualidad/2012/03/09/la-importancia-de-las-estrategias-de-ti-en-las-empresas/

Hernández, S., Fernández, C. y Baptista, P. (2010). *Metodología de la investigación*. (5.° edición). México: Mac Graw Hill.

Network Word. (2008). *Las diez áreas de TI con mayor demanda profesional*. Recuperado de http://www.networkworld.es/mundo-profesional/las-10-areas-ti-con-mayor-demanda-profesional

Pinto, C. (2009). *Formación de capital humano en el sector de TIC en Costa Rica*. México: Flacso.

Revista IT Now. (2015). *Pueden los departamentos de TI ser resilientes?* Recuperado de http://revistaitnow.com/2015/04/seguridad/pueden-los-departamentos-ti-ser-resilentes/

Tirado, J. (2000). *La demanda de expertos en seguridad IT supera la oferta*. Recuperado de http://revistaitnow.com/2013/04/seguridad/la-demanda-de-expertos-en-seguridad-it-supera-la-oferta/

Anexos

Instrumento de la investigación

Entrevista para conocer la percepción sobre la necesidad y el perfil de los profesionales en seguridad informática en Costa Rica.

Introducción:

La presente entrevista tiene como finalidad obtener su percepción sobre la necesidad que existe en las empresas nacionales, de contar con personal especializado en el área de seguridad informática y sobre los perfiles académicos que debe poseer este tipo de profesionales, de manera que se contribuya con la competitividad laboral del sector.

Instrucciones:

A continuación se le leerán una serie de preguntas que se le solicita responder de forma clara y detallada, de acuerdo con su experiencia y sus vivencias en relación con el tema. En sus respuestas puede extenderse hacia otros temas que considere necesarios, profundizar en áreas que considera más relevantes que otras y referirse incluso a temas que no se le han consultado, pero que estima pertinentes.

Durante la entrevista, el investigador podría realizarle consultas adicionales, con la finalidad de aclarar dudas o ampliar sobre nuevos puntos de vista, y tomará notas de lo conversado para un mejor registro y análisis posterior de los datos.

1. Por favor refiérase brevemente a su formación académica y a sus funciones laborales que lo califican como experto en materia de seguridad informática o como especialista en áreas de TI.

2. En su posición laboral actual, ¿contrata usted personal con formación técnica en el área de seguridad informática? Considera que es una plaza laboral indispensable en su empresa?

3. Cuando intenta contratar personal en esta área, ¿le resulta una tarea sencilla o es complicado encontrar personal especializado o competente que satisfaga sus necesidades en el área?

4. A corto plazo, ¿considera usted que las empresas en Costa Rica tendrán una orientación que las obligue a contratar profesionales con una formación técnica o un grado de bachillerato a nivel universitario en materia de seguridad informática?

5. Cuando se refiere a la formación técnica (en oposición a los profesionales que cuentan con un grado universitario de bachillerato), en su opinión, ¿cuántos años de estudio o cuántos cursos especializados considera que debió aprobar un estudiante para tener una formación de calidad?

6. De acuerdo con su experiencia, ¿le parece que el personal técnico en seguridad informática con el que ha trabajado hasta la fecha cuenta con las competencias laborales que se requieren actualmente en las empresas y organizaciones?

7. Si su respuesta es afirmativa, por favor señale las razones; si es negativa, por favor refiérase a las debilidades formativas a nivel académico o de competencias profesionales con las que no cuenta ese personal.

8. Si tuviera que diseñar una propuesta para un centro educativo que le consulte sobre el perfil profesional deseable en el mercado para formar un profesional técnico de calidad en seguridad informática, ¿cuál sería su recomendación? ¿Podría usted señalar las áreas en las que se debe especializar y los conocimientos técnicos indispensables?