Formación profesional | Reflexiones Y Saberes
Fundación Universitaria Católica del Norte, 6, 34-47
ISBN-2389-7511 (en línea)

¿Cómo citar el artículo?

Guevara Calume, R. C., Gómes Jaramillo, S. & Sepúlveda, J. M. (2017). Formación profesional en el campo de la seguridad informática, a través de sus componentes básicos. *Revista Reflexiones y Saberes,* (6), 34-47

Formación profesional en el campo de la seguridad informática, a través de sus componentes básicos

Vocational training in the field of computer security, through its basic components.

Roberto Carlos Guevara Calume
Ingeniero de Sistemas
Magister en Automatización y Control Industria,
Especialista en Redes Corporativas e Integración de Tecnologías,
PhD(c) en proyectos TIC,
Correo electrónico: rcguevara@ucn.edu.co

Sebastián Gómez Jaramillo
Ingeniero de Sistemas
Magister en Ingeniería – Ingeniería de Sistemas
PhD (c) en Ingeniería
Correo electrónico: sebastian.gomez.j@gmai.com, sgomezja@tdea.edu.co

Jorge Mauricio Sepúlveda
Ingeniero de Sistemas,
Especialista en Redes Corporativas e Integración de Tecnologías,
jsepulveda@uniremington.edu.co
PhD(c) en proyectos TIC,

Tipo de artículo: Articulo corto de reflexión

Formación profesional | Reflexiones Y Saberes
Fundación Universitaria Católica del Norte, 6, 34-47
ISBN-2389-7511 (en línea)

Resumen

La importancia de capacitar personas en el área de la seguridad informática es latente debido a las investigaciones que se han hecho al interior de las organizaciones, donde la mayoría han manifestado haber sido víctimas de al menos un ataque informático. En el presente trabajo, se hace un recorrido tanto a nivel local como global, en donde se evidencian los principales ataques recibidos por las organizaciones, así como la importancia de poder estar preparados para contrarrestarlos. Posteriormente se presentan los antecedentes en el caso colombiano a nivel de formación profesional (de postgrado) en el área de seguridad de la información, con los diferentes perfiles de cada uno de los programas. Finalmente, se identifican unas premisas que permiten caracterizar los componentes bases que debe tener un profesional en el área de seguridad de la información, tanto a nivel de gestión de la información, en el nivel defensivo, ofensivo y legal.

Palabras clave: seguridad informática, componentes básicos, oferta educativa

Abstract

Abstract
The importance of training in the area of computer security is latent because of the research that has been done within organizations, where most have indicated they were victims of at least one computer attack. In this paper, a tour is done both locally and globally, where the main attacks received by organizations are evident, and the importance of being able to be prepared to counter them. Subsequently the backgrounds are presented in the Colombian case at the level of vocational training (postgraduate) in the area of information security, with the different profiles of each of the programs. Finally, some premises that allow characterization of the base components should have a professional in the area of information security are identified, both in terms of information management, on the defensive, offensive and legal level.

Keywords: computer security, Basic components Educative offer

Introducción

Aunque existen Software y Hardware orientados al tema de evaluar la seguridad de los sistemas de información, así como defender los sistemas de información, también es cierto que se requiere el conocimiento formal del talento humano cualificado para articular estas herramientas entre sí. Esto permite la identificación y tratamiento de riesgos y amenazas, así como gestionarlos de una forma integral, basados en los principios fundamentales de la seguridad de la información y la comunicación (Gómez, 2008).

Por este motivo, desde el punto de vista académico es importante diseñar programas de formación avanzada que obedezcan a estos principios. Teniendo como fin la formación de personal competente en esta área del conocimiento desde un ámbito profesional, sin dejar de reconocer otras maneras no formales de abordar el problema de la seguridad informática.
En Colombia, las carreras universitarias en Tecnologías de la Información solo incluyen la seguridad de la información en algunas asignaturas de forma complementaría u opcional. Sin embargo, la educación no formal, representada en cursos, seminarios y diplomados, orientan la formación en la seguridad de la información de una forma dispersa, integrando temas que no son

Formación profesional | Reflexiones Y Saberes
Fundación Universitaria Católica del Norte, 6, 34-47
ISBN-2389-7511 (en línea)

secuenciales, y que, finalmente, quedan desarticulados en cuanto a la formación integral y secuencia que debe de aplicarse a la seguridad de la información.
Darle el respectivo nivel de continuidad a la seguridad de la información y a las tecnologías que permiten dicho procesamiento, requiere que componentes importantes como la cultura, concientización, elementos tecnológicos, normas, herramientas de gestión y el recurso humano, trabajen de forma conjunta, para lograr un sistema de gestión de seguridad de la información integral, y con orientación hacia la visión, misión y objetivos estratégicos de una empresa u organización.

1. Situación Problemática

La cantidad e importancia de la información en las organizaciones llevan a tener un interés claro en su protección. Esto se presenta debido al alto número de ataques que se presentan día a día, no solo a nivel internacional sino en el ámbito local. Dichos ataques se dan en diferentes niveles, desde entidades importantes como la registraduría, la policía y la misma presidencia (El Heraldo, 2011). Donde los atacantes pueden extraer datos personales de cientos de funcionarios de la policía, publicarlos en Internet de forma arbitraria sin ningún tipo de control o restricción, exponiendo así, información sensible de funcionarios públicos en la red internet. También es bueno señalar que las pequeñas y medianas empresas están expuestas a ser atacadas debido que poseen información sensible.

La Asociación Colombiana de Ingenieros de Sistemas (ACIS), le da un interés especial al tema, realizando cada año la Encuesta Latinoamericana de Seguridad de la Información, que en el caso del año 2015 se denominó Nuevos retos, nuevas realidades (Cano & Saucedo, 2015).

La encuesta fue aplicada a 270 personas de diferentes nacionalidades que se encuentran en sectores estratégicos, como en el sector público, telecomunicaciones, la banca, el educativo, entre otros. Las personas encuestadas tenían en su mayoría la función de velar por la protección de la información empresarial, así como en el seguimiento de las prácticas en materia de seguridad.

El 29% de los encuestados manifestaron haber recibido entre uno y tres incidentes durante el año anterior, mientras el 36,4% recibieron más de cuatro incidentes. Preocupa que el 26% de las compañías no tenían la información sobre dichos incidentes. Sin embargo, este porcentaje disminuyó significativamente con respecto a la misma pregunta en los años anteriores. Por su parte los ataques han aumentado, pasando de un 29% a un 36,4% en las compañías que tuvieron más de 4 incidentes de seguridad.

Los ataques más recurrentes correspondieron a la instalación de Software no autorizado, a los virus/caballos de Troya, al phishing y a accesos no autorizados al web.

Uno de los inconvenientes y oportunidades para la mejora en las empresas regionales y a nivel de Colombia, es que algunas aún tienen la idea de que la seguridad de la información a nivel integral, solo es para las grandes empresas y multinacionales, incrementando con este tipo de pensamientos, el riesgo de ser víctimas de ataques informáticos dirigidos o al azar por parte de delincuentes informáticos novatos. Muchas de las pequeñas y medianas empresas de nuestro país y región, cuentan simplemente con controles básicos de seguridad, como lo es un Antivirus, y un Sistema de Filtrado de paquetes "Firewall", los cuales brindan una falsa sensación del estado de la seguridad de la información, ya que solo son dos componentes o eslabones que componen la cadena de la seguridad de la información, y la protección de los datos.

Otro aspecto de gran relevancia, son las tendencias actuales y a un futuro de corto plazo, en lo que respecta a las transacciones, pagos bancarios y de servicios. Un gran porcentaje de personas

Formación profesional | Reflexiones Y Saberes
Fundación Universitaria Católica del Norte, 6, 34-47
ISBN-2389-7511 (en línea)

como ejecutivos, profesionales, gerentes de empresa, empleados, estudiantes, entre otros, usan las tecnologías, portales Web, pasarelas de pago y la banca electrónica para hacer sus pagos de cuentas de teléfono celulares, servicios públicos, pagos de nómina, pago a proveedores, seguridad social, comprar productos, adquirir cursos, hacer apuestas, entre otros. El dinero electrónico es una tendencia representativa, y se requiere de profesionales con un conocimiento integral que tenga dentro de su alcance las medidas preventivas, leyes, y tecnologías necesarias para garantizar y apoyar a que este tipo de transacciones sean seguras y no esté en altos niveles de riesgo frente a las amenazas, fraudes y ataques informáticos que puedan afectar los niveles de Integridad, Disponibilidad, Autenticidad y Confidencialidad de la información y los sistemas informáticos que la contienen, trasportan y procesan (Morón Lema, 2002)

Finalmente, en Colombia se creó el Centro Cibernético Policial (CCP) el cual en el año 2013 respondió ante 1647 ataques, 62% de estos fueron realizados hacía ciudadanos particulares, el 21% a entidades del sector bancario y el resto a diferentes entidades, principalmente pertenecientes a sectores del gobierno. Las tendencias de estos ataques fueron los códigos maliciosos, el phishing (Suplantación de identidad) y el robo de información (Symantec, 2014).

2. Antecedentes

Según el informe de ACIS (Cano & Saucedo, 2015) también se cuestionó el papel de la academia en la formación de profesionales en seguridad de la información. Los resultados arrojaron que el 44,6% considera que se ofrecen programas de grado y/o posgrado formales en el área, pero también consideran en alto número que el nivel de investigación en el tema es escasa o insuficiente. Otro de los hallazgos referentes al papel de la academia responde a la necesidad de laboratorios e infraestructura adecuada para soportar los cursos especializados, también ampliar el número de alianzas con proveedores de tecnologías de seguridad.
A partir de este antecedente se muestra a continuación la oferta de programas en la región correspondientes a solucionar la necesidad identificada.

2.1. Oferta de Programas

A nivel profesional en la formación de posgrado en seguridad de la información, la oferta de programas de especialización en esta área son relativamente limitados a nivel de la regional, en el departamento de Antioquia se encontraron los siguientes programas descritos en la tabla 1 (MinEducación, 2016).

Formación profesional | Reflexiones Y Saberes
Fundación Universitaria Católica del Norte, 6, 34-47
ISBN-2389-7511 (en línea)

Institución	Denominación Programa	Perfil o Descripción
Tecnológico de Antioquia	Especialización en Seguridad de la Información (Tecnológico de Antioquia, 2015)	Profesional proactivo en la prevención y neutralización de riesgos que puedan afectar la seguridad de la información así como aplicar métodos para la recuperación de la información ante incidentes de seguridad, que se puedan presentar en las diferentes organizaciones, de igual manera ser líder en la implementación, desarrollo y aplicación de técnicas, métodos y herramientas orientadas a brindar protección a la información empresarial.
Universidad San Buenaventura	Especialización en Seguridad Informática (Universidad de San Buenaventura, 2015)	Busca dar solución a la necesidad existente sobre la gestión de la seguridad de la información, teniendo como precedente, las amenazas y vulnerabilidades que se presentan en los sistemas informáticos de las organizaciones. Áreas de Desempeño • Implementar controles de seguridad • Gestionar las variables administrativas y operativas que inciden en el control de los riesgos

Formación profesional | Reflexiones Y Saberes
Fundación Universitaria Católica del Norte, 6, 34-47
ISBN-2389-7511 (en línea)

Universidad Pontifica Bolivariana	Especialización en Seguridad Informática (Universidad Pontifia Bolivariana, 2015)	Todas las organizaciones en sus procesos de negocios utilizan Internet como elemento primordial en su operación. Cuanto más se utilice la Red para los procesos de negocio, mayor es la necesidad de que esta red garantice altos niveles de confiabilidad y disponibilidad de la información que viaja a través de ella. El perfil es: • Aplicar y promover metodologías actualizadas que conduzcan a la práctica de una cultura de seguridad informática. • Capaz de discernir entre las ventajas y desventajas asociadas con el diseño y administración de políticas de seguridad. • Diseñar estrategias que puedan garantizar la seguridad de los recursos informáticos.
Corporación Universitaria Remington	Seguridad de la Información (UNIREGMINTON, 2015)	Profesional preparado en cuatro frentes claves para la seguridad de la información: las auditorias técnicas intrusivas (hacking ético), defensa por capas (defensa en profundidad), gestión de la seguridad de la información y la computación forense.
Católica del Norte Fundación Universitaria	Especialización en Gestión de Seguridad y Riesgo Informático (Norte, 2016)	Profesional que dispone de las competencias para liderar la planificación e implantación de estrategias y mejores prácticas asociadas con la protección de los recursos de información y componentes tele-informáticos en las organizaciones, tendientes a mitigar y/o evitar que se materialicen eventos o amenazas

Formación profesional | Reflexiones Y Saberes
Fundación Universitaria Católica del Norte, 6, 34-47
ISBN-2389-7511 (en línea)

Instituto Tecnológico Metropolitano	Magíster en Seguridad Informática (ITM, 2016)	Con Énfasis en Gestión de Incidentes de Seguridad de la Información orientado hacia la profundización del dominio técnico y de los desarrollos teóricos modernos que subyacen en esta práctica profesional, para la solución de problemas reales en las organizaciones.

Se destaca que la oferta se da tanto en instituciones públicas como privadas, así como en modalidad presencial y virtual. Finalmente, es importante que también ya se está ofreciendo una maestría en el área.

A nivel nacional, existen otros programas de especialización y maestría, destacándose tres programas en este nivel. La maestría del ITM, la Maestría en Seguridad de la Información de la Universidad de los Andes y la Maestría en Ciberseguridad y Ciberdefensa de la Escuela Superior de Guerra.

2.2. Premisas identificadas

Con respecto a los antecedentes en los programas ofertados a nivel regional y nacional, se diseñaron unas premisas y objetivos buscados que debe tener un programa de postgrado en el área de seguridad de la información. Las cuales también tuvieron en cuenta la opinión de expertos temáticos y docentes:

- Seguridad de la información orientada al campo productivo y de servicios.
- Habilidades y conocimientos en a nivel ofensivo, defensivo, legal y a nivel de gestión.
- Claridad en la visión general de la seguridad de la información, y el impacto que esta tiene en la tecnología presente y futura.
- Conocer los diferentes tipos te atacantes informáticos, con las respectivas técnicas de ataque y las herramientas con que las materializan.
- Conocer y aplica las normas internacionales, legislaciones y buenas prácticas relacionadas con la seguridad de la información.

Formación profesional | Reflexiones Y Saberes
Fundación Universitaria Católica del Norte, 6, 34-47
ISBN-2389-7511 (en línea)

3. Metodología – Identificación de componentes bases

Para la identificación de los componentes bases, se tuvieron en cuenta los antecedentes y las premisas identificadas, además del aspecto legal para la generación de talento humano idóneo en esta área.A continuación se describe este componente legal, los perfiles esperados y la descripción de cada uno de los componentes bases, que conformarían la estructura curricular.

La creación de la estructura curricular parte de la idea que los futuros protectores de datos y sistemas son las personas que se están capacitando en la actualidad, por lo tanto es fundamental para las universidades promover entrenamiento en seguridad y aseguramiento de la información (White, Hewitt, & Kruck, 2013).

3.1. Componentes Legales

En Colombia se resaltan dos documentos nacionales que tratan sobre la Seguridad de la Información, el primero es el Documento Conpes 3701 (DNP, 2011)que indica los lineamientos de política para ciberseguridad y ciberdefensa. El cual busca desarrollar una estrategia nacional para contrarrestar el incremento de amenazas informáticas que afectan al país. El principal problema encontrado trata sobre la capacidad actual del Estado para enfrentar amenazas, y la inexistencia de una política sobre esto.

Por parte de la ley colombiana, se encuentra la Ley 1723 de 2009 (Congreso de Colombia, 2009)que busca judicializar y penalizar lo relacionado con delitos informáticas. Creando un bien jurídico tutelado denominado “De la protección de la información y de los datos”. En esta ley se destacan artículos como:

- Acceso abusivo a un sistema informático
- Obstaculización ilegítima de sistema informático o red de telecomunicación
- Interceptación de datos informáticos
- Daño Informático
- Uso de Software Malicioso
- Violación de Datos Personales
- Suplantación de sitios web para capturar datos personales
- Hurto por medio informático
- Transferencia no consentida de activos
- Entre otros.

3.2. Componentes Bases

Se definieron unos componentes bases que puedan responder a perfiles importantes para un egresado de un postgrado en Seguridad de la Información, dos generales que responden a la gestión de la información y a las generalidades de la seguridad, posteriormente dos que tratan sobre el ataque y la defensa, denominados seguridad a nivel ofensivo y seguridad a nivel defensivo.

3.2.1. Componente Generalidades de la Seguridad de la Información

Contiene todos los conocimientos básicos que el especialista debe de comprender en lo que

Formación profesional | Reflexiones Y Saberes
Fundación Universitaria Católica del Norte, 6, 34-47
ISBN-2389-7511 (en línea)

respecta a la seguridad de la información, y la seguridad informática, tales como los fundamentos de la seguridad de la información, la arquitectura segura de redes informáticas, la seguridad asociada a los sistemas operativos, las amenazas y riesgos tecnológicos a los cuales está expuesta la información, y la fundamentación de los criterios generales de la seguridad de la información, como los son: La Disponibilidad, Integridad y Confidencialidad de la información.

Los anteriores conceptos son fundamentales para comprender la importancia, impacto, alcance y objetivos de la seguridad de la información y su aplicación en las tecnologías de la información y en el procesamiento y almacenamiento de datos en medios digitales.

3.2.2. Componente Gestión de la información

Suministra todos los conocimientos necesarios para conducir al especialista en seguridad de la información, a comprender de una forma estructurada como se hace la gestión de la seguridad de la información, aplicando estándares internacionales de Sistemas de Gestión de la Seguridad de la Información (SGSI), tales como los pertenecientes a la familia ISO 27001 (ICONTEC, 2006), dentro de los cuales se incluyen normas importantes tales como:

- Norma ISO Descripción
- ISO 27001 Esla norma principal de la familia 27000, y contiene los requisitos que debe de cumplir una organización para obtener la certificación del SGSI bajo la norma ISO 27001.
- ISO 27002 Guía de buenas prácticas que describe los objetivos y criterios de control que deben de tener una organización para implementar y certificar el SGSI bajo la norma ISO 27001.
- ISO 27003 Es una guía que orienta a una organización para el diseño y montaje del SGSI
- ISO 27005 Es una guía que proporciona todas las directrices para la realización del análisis de riesgos, el cual es un componente base y de gran importancia para la implementación del SGSI.

Para este componente se ven asignaturas en las cuales se le suministran al especialista en seguridad de la formación los conceptos y técnicas para implementar un Sistema de Gestión de Seguridad de la Información (SGSI), con sus componentes principales tales como:

- Gestión Integral del Riesgos
- Realización de políticas de seguridad y documentación del SGSI
- Análisis de Activos tecnológicos
- Gestión de Incidentes
- Gestión de Continuidad del Negocio
- Gestión Integral de Controles
- Declaración de aplicabilidad

Además el estudiante especialista en seguridad de la información aprenderá de forma estructurada como se realiza una pre-auditoria y auditoría a un Sistema de Gestión de Seguridad de la Información (SGSI), con criterios y bases de auditorías soportados en la norma técnica Colombiana NTC-ISO 27001.

Finalmente este componente contiene asignaturas donde se mencionan los criterios y leyes colombianas que están relacionadas con los delitos informáticos y en general con el uso de las tecnologías de la información, lo cual es un aspecto importante y relevante para la gestión integral de la seguridad de la incoación en una empresa u organización.

3.2.3. Componente Seguridad a Nivel Defensivo"

Formación profesional | Reflexiones Y Saberes
Fundación Universitaria Católica del Norte, 6, 34-47
ISBN-2389-7511 (en línea)

Suministra todos los conocimientos necesarios para conducir al estudiante a comprender desde una forma básica, hasta las tendencias de las tecnologías de la información más avanzadas en nuestros días, a desarrollar habilidades conceptuales, prácticas y técnicas para implementar mecanismos de defensa de una forma modular en los sistemas de información. El componente en mención aborda las técnicas de defensa de redes informáticas más representativas y necesarias, haciendo uso del Modelo de Defensa en Profundidad, en el cual se aplican de forma conceptual y práctica, técnicas de defensa tales como: Sistemas de Filtrado de Paquetes Firewall, Sistemas detectores/preventores de Intrusos, Servidores de redes privadas VPN, Sistemas trampa Honeypots, Sistemas Unificados de Amenazas y técnicas aplicadas de criptografía, estenografía y certificados Digitales (Paar & Pelzl, 2010). Lo anterior complementado con la aplicación de modelos de defensa de sistemas informáticos basados en las nuevas tendencias de las tecnologías de la información, tales como las redes inalámbricas el protocolo IPV6, la computación en la nube y la computación aplicada a los dispositivos móviles.

Los anteriores conceptos son fundamentales para complementar las bases de la seguridad de la información de una forma más práctica, la cual se puede ver representada en la implementación de modelos defensivos por capas (Modulares) de sistemas y redes informáticas que suministren niveles aceptables que garanticen la Disponibilidad, Confidencialidad e Integridad para la información digital (Santos, 2008).

3.2.4. Componente Seguridad a Nivel ofensivo

suministra todos los conocimientos a nivel conceptual, técnicos y metodológicos necesarios para conducir al estudiante a comprender de una forma estructurada las formas en que los atacantes informáticos y/o Auditores de seguridad Éticos pueden llevar a la práctica ataques contra las redes y sistemas de información. Durante el desarrollo de las asignaturas de este componente, el estudiante desarrolla conceptos y habilidades para comprender las clases de atacantes informáticos que existen, con su respectiva evolución hasta nuestros días, los tipos de visibilidad y de test de seguridad que se pueden ejecutar al evaluar la seguridad de un sistema informático, además aprenderá sobre las técnicas de ataque más usadas por los delincuentes informáticos tales como:

- Ataque de Negación de Servicios Distribuido
- Malware
- Virus Troyanos
- Keyloggers
- Ataques por Fuerza Bruta
- Cracking de Password
- Scanning de Puertos
- Análisis de vulnerabilidades
- Sniffers
- Phising y Phraming.

En este componente todos los conceptos relacionados con las técnicas y herramientas usadas por los atacantes informáticos se verán de forma secuencial y ordenada, aplicando metodologías y estándares de auditorías de seguridad del tipo Hacking Ético y/o PenetrationTesting en sistemas, redes informáticas y dispositivos móviles, donde de forma secuencial se aplican todas las fases de una auditoria de seguridad ética y ejecutada por profesionales de la seguridad de la información, comenzando por fase de recolección de información (InformationGathering), hasta llegar a la fase Post-explotación y presentación de reportes técnicos y ejecutivos de la respectiva auditoria y/o evaluación de seguridad (Santos, 2008).

Formación profesional | Reflexiones Y Saberes
Fundación Universitaria Católica del Norte, 6, 34-47
ISBN-2389-7511 (en línea)

De forma completa las fases de una auditoría técnica de seguridad del tipo Hacking Ético y/o PenetrationTesting que se enseñan en el componente "Seguridad de la información Nivel Ofensivo" son:

Fase 1: Footprintig Recolección de Información
Fase 2: Scanning de Puertos y Enumeración
Fase 3. Análisis de Vulnerabilidades
Fase 4: Explotación
Fase 5: Post-Explotación
Fase 6: Presentación de Reportes

Teniendo presente que muchos vectores relacionados con los atacantes y técnicas de ataque que afectan los sistemas de información van evolucionando, se complementan los conocimientos en el componente "Seguridad de la información Nivel Ofensivo" haciendo inclusión de temas en las asignaturas de este componente en lo que respecta a la seguridad de la información orientada a las aplicaciones web, ya que es un vector de ataque que en los últimos años se ha incrementados de forma considerable en lo que respecta al desarrollo e implementación de aplicaciones web, y la gran cantidad de ataques que sufren este tipo de aplicaciones.

En las asignaturas relacionadas con la seguridad web se suministran todas las bases, fundamentos, metodologías y conceptos sobre la arquitectura de una aplicación web dinámica, donde se hace énfasis en los riesgos y amenazas a las cuales están expuestas este tipo de aplicaciones, las técnicas de intrusión más comunes, y la forma de asegurar una aplicación Web transaccional. Las técnicas de ataque y/o amenazas tecnológicas que se aprenderán en las asignaturas relacionadas con seguridad web son:

- Fuerza Bruta
- Ejecución de Comandos
- File Inclusión
- PathTraversal
- XSS (Cross Site Scripting)
- SQL Injection
- CSRF-XSRF

De forma trasversal a los conocimientos técnicos que se suministran al especialista en seguridad de la información en lo que respecta a las auditorias de seguridad técnicas orientadas al tema ofensivo, se aplican estándares de auditorías técnicas de seguridad usadas a nivel internacional, tales como:

- OWASP TOP 10
- NIST-
- Technical Guide to Information Security Testing and Assessment
- Open Source Security Testing Methodology Manual (OSSTMM)

Una vez que se obtienen los conceptos teóricos, prácticos y metodológicos relacionados con las evaluaciones de seguridad del tipo Hacking Ético y/o PenetrationTesting y se conocen las herramientas y técnicas con que los delincuentes informáticos atacan los sistemas, redes y en general la infraestructura tecnológica de una empresa u organización, se suministra al estudiante todos los conceptos relacionados con la Informática Forense y el Análisis de la Evidencia Digital, con el objetivo de realizar auditorías orientadas al tema de investigación forense, basados en la evidencia digital.

Formación profesional | Reflexiones Y Saberes
Fundación Universitaria Católica del Norte, 6, 34-47
ISBN-2389-7511 (en línea)

En la aplicación de Computación Forense y Análisis de Evidencia Digital, se orienta al especialista en seguridad de la información a que aplique todos los conceptos obtenidos en las técnicas de ataque y auditorías técnicas intrusivas (Scambray & MCclure, 2008), pero ya desde el punto de vista de un auditor-analista forense que responde directamente a incidentes y/o delitos cometidos usando las tecnologías de la información, el cual basa todo su análisis en la evidencia digital obtenida de situaciones comunes relacionadas con las amenazas tecnológicas tales como:

- Ataques y delitos relacionados con las tecnologías de la información
- Espionaje Industrial y Económico
- Hackitivismo

Aplicación transversal en cada uno de los componentes de la especialización en seguridad de la Información.

3.2.5. Componente transversal

En el programa de especialización en seguridad de la información se aplican de forma trasversal dos componentes descritos como:

Buenas Prácticas y Estándares Internacionales: De forma trasversal a los conocimientos técnicos que se suministran durante el desarrollo de la especialización en seguridad de la información, se aplican estándares y aplicación de buenas prácticas relacionadas con la seguridad de la información tales como:

- OWASP TOP 10
- Familia ISO 27000
- NIST- Technical Guide to Information Security Testing and Assessment
- Open Source Security Testing Methodology Manual (OSSTMM)

Leyes y Legislación sobre la Seguridad de la Información en Colombia: De forma trasversal a los conocimientos teóricos y prácticos que se suministran durante el desarrollo de la especialización en seguridad de la información, se aplican y se enseñan al especialista en seguridad las bases sobre las leyes colombianas que están relacionadas con los delitos informáticos y en general con el uso de las tecnologías de la información. Para el caso del programa de especialización en seguridad de la información se orientara al estudiante sobre el conocimiento y aplicación de las siguientes leyes:

- Ley 1273 de 2009 "De la protección de la información y de los datos"
- Ley Estatutaria 1581 “Por la cual se dictan disposiciones generales para la protección de datos personales”.

De forma consecuente con el objetivo de asegurar el desarrollo de las competencias a nivel técnico y a nivel investigativo se diagrama en el siguiente gráfico la interrelación y articulación entre currículo del programa de especialización en seguridad de la información, detallando en dicho grafico cada componente del programa de especialización con sus respectivas asignaturas y la relación de estas con las competencias que se desarrollan durante el programa de especialización

3.2.6. Componente en Investigación

Si bien es claro que no se establece que las especializaciones sean de carácter investigativas, la solución de problemas específicos y la implantación de innovaciones en los campos de actuación del especialista, implican la competencia investigativa para la formulación de proyectos para la solución de necesidades, en especial en el área de la seguridad de la información, donde hay mucho que investigar y aplicar.

Formación profesional | Reflexiones Y Saberes
Fundación Universitaria Católica del Norte, 6, 34-47
ISBN-2389-7511 (en línea)

| Conclusiones

La estructura principal de la especialización en seguridad de la Información, se basa en cuatro componentes, los cuales organizan el programa y el estudio de la seguridad de una manera secuencial.

- Bases de la Seguridad de la Información
- Seguridad Informática Ofensiva
- Seguridad Informática Defensiva
- Gestión de la Seguridad de la Información.

Estos cuatro componentes siguen los siguientes lineamientos

- Buenas Prácticas
- estándares internacionales
- Leyes y Legislación sobre la seguridad de la información

La estructura propuesta para el desarrollo de programa en la Especialización en seguridad de la información, surge de un proceso sistemático de investigación del estado del arte en la seguridad de la información, haciendo énfasis en lo profesional y académico, apoyando en la experiencia docente, con esto se garantiza que el programa presentado cubre en forma trasversal todos los aspectos relacionados con la seguridad de la información, a través de sus componentes y lineamientos.

Por lo tanto se hace necesario tener en Colombia instituciones universitarias, que ofrezcan a los profesionales carreras universitarias a nivel de Posgrado, donde se formen profesionales capacitados, en todo lo relacionado con la seguridad de la información, teniendo alcances y componentes claves, tales como: la seguridad ofensiva, la seguridad defensiva, la computación forense, la atención ante incidentes relacionados con la tecnología y la gestión de la seguridad, las cuales fortalezcan y formen profesionales integrales en seguridad de la información, con las suficientes competencias para afrontar los retos y exigencias que tiene el mercado tecnológico y las empresas a nivel nacional e internacional, frente a todo el ciclo de asegurar los sistemas de información, y de integrar a su grupo de trabajo profesionales capacitados, que ayuden a mantener en las empresas y

Formación profesional | Reflexiones Y Saberes
Fundación Universitaria Católica del Norte, 6, 34-47
ISBN-2389-7511 (en línea)

Referencias

Cano, J., & Saucedo, G. (2015). *VII Encuesta Latinoamericana de Seguridad de la Información.* Bogotá: ACIS.

Congreso de Colombia. (2009). *Ley 1273 de 2009.* Bogotá.

DNP. (2011). *Documento Conpes 3701*. Bogotá: Dirección Nacional de Planeación.

El Heraldo. (16 de Agosto de 2011). Los golpes de los 'hackers'. *El Heraldo.*

Gómez, A. (2008). Principios de la seguridad informática. En *Enciclopedia de la Seguridad Informática* (págs. 37-69). España: RA-MA Editorial.

ICONTEC. (2006). *Norma Técnica Colombiana NTC-ISO/IEC 27001.* Bogotá: Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC).

ITM. (2016). *Maestría en Seguridad Informática.* Obtenido de Instituto Tecnológico Metropolitano: http://posgrados.itm.edu.co/mseguridadinfo.html

MinEducación. (2016). *Búsqueda de Programas de Instituciones de Educación Superior.* Obtenido de Sistema Nacional de Información de la Educación Superior: http://snies.mineducacion.gov.co/consultasnies/programa#

Morón Lema, E. (2002). *Internet y Derecho Penal: Hacking y otras Conductas Ilícitas en la Red.* Aranzadi.

Norte, C. d. (2016). *Especialización en Gestión de Seguridad y Riesgo Informático.* Obtenido de Católica del Norte Fundación Universitaria: http://www.ucn.edu.co/programas-academicos/Paginas/posgrados/especializacion-gestion-seguridad-riesgos-informatico.aspx

Paar, C., & Pelzl, J. (2010). *Understanding Cryptography.* Berlin: Springer Berlin Heidelberg.

Philipp, A., & Cowen, D. (2010). Forensic Investigation Techniques. En *Hacking Exposed Computer Forensics* (págs. 128-338). San Francisco: McGrawHill.

Santos, O. (2008). Defense-in-Depth Applied. *End-to-End Network Security: Defense-in-Depth*, 209-337.

Scambray, J., & MCclure, S. (2008). *HACKING EXPOSED WINDOWS SECURITY SECRETS & SOLUTIONS.* United States: McGrawHill.

Symantec. (2014). *Tendencias de Seguridad Cibernética en América Latina y el Caribe.* Organización de los Estados Americanos.

Tecnológico de Antioquia. (2015). *Especialización en Seguridad de la Información.* Obtenido de Tecnológico de Antioquia: http://www.tdea.edu.co/index.php/facultades/facultad-de-ingenieria/especializacion-en-seguridad-de-la-informacion

UNIREGMINTON. (2015). *Seguridad de la Información.* Obtenido de UNIREGMINTON: http://www.uniremington.edu.co/seguridad-de-la-informacion.html

Universidad de San Buenaventura. (2015). *Posgrados - Esepcialización en Seguridad Informática.* Obtenido de Universidad de San Buenaventura: http://www.usbmed.edu.co/index.php/especializacion-en-seguridad-informatica

Universidad Pontifia Bolivariana. (2015). *Especialización en Seguridad Informática.* Obtenido de Universidad Pontifia Bolivariana: http://www.upb.edu.co/portal/page?_pageid=1054,43349789&_dad=portal&_schema=PORTAL

White, G., Hewitt, B., & Kruck, S. (2013). Incorporation Global Information Security and Assurance in I.S Education. *Journal of Information Systems Education, 24*(1), 11-16.