# Importancia del Aprendizaje de Ciberseguridad ante los Riesgos de las Tecnologías de Información

# The Importance of Cybersecurity Regarding the Risks of the Information Technologies

Universidad Latina de Costa Rica

Autor: ELÍAS CARABAGUÍAZ GONZÁLEZ

sinistar491@gmail.com

## RESUMEN

La ciberseguridad es un área de la informática que está creciendo tanto en su aprendizaje como en su demanda profesional. Desafortunadamente, su estudio y su práctica no están estandarizados en ningún ente educativo, de forma que el aprendizaje viene a partir de certificaciones y grados académicos, lo cual resulta muy tardío. Debido al clima organizacional mundial y la necesidad de proteger la información sensible de las empresas, se ha despertado una demanda de especialistas en la materia que no se puede cubrir debido a la carencia de conocimiento y experiencia.

El presente artículo explica el proceso de investigación sobre las bases de aprendizaje actuales respecto del tema de la seguridad informática, en comparación con la demanda actual de profesionales. La investigación busca sentar las bases, requerimientos para proponer un

diseño instruccional y establecer una ruta profesional en grados académicos posteriores y sacar profesionales capacitados dentro del ámbito de la informática.

**ABSTRACT**

Cybersecurity is a growing area in computer science, from its learning to its professional demand. Unfortunately, the knowledge acquisition and its practice are not standardized in no academic degree, and thus the aspirant must learn it very late in its career or to opt for certification programs with no fundamentals or knowledge background. Due to the increasing need to secure information from companies, corporation and even governments, the demand for security specialists are on the rise and institutions are not able to meet those demands, due to lack of knowledge or experience.

This article will provide insight in the investigation that took place to study the overall and popular knowledge among computer engineers regarding cybersecurity, and stablish a comparison on what companies are looking for nationwide and worldwide. Once the investigation is completed, a proposal for an instructional design in which will provide the fundamentals in a way that an aspirant can obtain the required knowledge and start a career path in cybersecurity.

**PALABRAS CLAVE**

- Seguridad
- Cybersecurity
- Informática
- Aprendizaje
- Learning
- Diseño instruccional
- Instructional Design
- Hacker

## INTRODUCCIÓN

La era actual es la de la información. A diferencia de otras épocas, el valor que tiene la información hoy en día, es muy alto. Esto se debe a que países, compañías y hasta organizaciones sin fines de lucro manejan una gran cantidad de información ya sea financiera, contable, de personas, procesos, resultados en el mercado y otros muchos. Es importante partir del hecho que la información junto con las telecomunicaciones ha dado forma al mundo contemporáneo. Debido a la que información se ha vuelto uno de los cimientos de una empresa, la pérdida de la misma puede comprometer el funcionamiento o su éxito. Esto hace que se vuelva sensible la adquisición de nuevas tecnologías a una empresa para tener un funcionamiento eficaz, ya que puede comprometer la integridad y la seguridad de su información.

La ciberseguridad es un área de la informática que ha venido en aumento, tanto en su aprendizaje como en su demanda profesional. El concepto que le da Feliu (2013) a la ciberseguridad "…consiste en la aplicación de un proceso de análisis y gestión de los riesgos relacionados con el uso, procesamiento, almacenamiento y transmisión de información o datos y los sistemas y procesos usados basándose en los estándares internacionalmente aceptados" (Feliu, 2013, pág. 6). Desafortunadamente su estudio y su práctica no están estandarizados en ningún ente educativo del país, de forma tal que el aprendizaje viene a partir de certificaciones y grados académicos superiores, lo cual resulta muy tardío a la hora de poner en práctica. Debido demanda a nivel mundial y la necesidad de proteger la información sensible de las empresas, se ha despertado a hacer requerimiento de especialistas en la materia que no se puede cubrir debido a la carencia de conocimiento y experiencia.

Según la revista *DarkReading* menciona que "Los tipos de ataques más populares a bases de datos son: Ataques de fuerza bruta, robo de credenciales privilegiadas, vulnerabilidades en servicios no utilizados de las bases de datos (*plugins*, extensiones, entre otros), Bases de datos sin mantenimiento o actualizaciones, inyecciones de SQL, robo de respaldos" (Higgins, 2008).

Lo anterior sin duda justifica el hecho que en el Programa de investigación Vertex Alma Mater, se considerara como uno de los temas o aristas de investigación la Ciberseguridad, Los esfuerzos por brindar un constructo cognitivo alrededor de éste son necesarios y tal vez más

aún, imperativos, máxime que se puede dotar a la Escuela de Ingeniería de Sistemas y a la Facultad de Tecnologías de Información y Comunicación, para su mejoramiento continuo. Vertex Alma Mater ha venido a ser un semillero de proyectos relacionados con la tecnología digital que se encuentran dentro de los conocidos como estado del Arte de los cuales la Cyberseguridad es uno de los más significativos.

Como parte de esta investigación, se identificó una que hay un existente déficit en el área de la ciberseguridad, esto se debe a que, a nivel nacional, no se puede satisfacer la demanda de profesionales en dicha área. Adicional a este problema, los profesionales en seguridad informática, no cuentan con un conocimiento estandarizado sobre la materia. Esto se debe a que, actualmente se recurre a capacitaciones laborales, certificaciones, o medios de dudosa procedencia para poder adquirir este conocimiento. Con la investigación objeto de este artículo, se buscó una propuesta para modernizar la forma en que se estudia la informática en el país tratando de fomentar la investigación de nuevas áreas poco exploradas de la computación e informática.

Basado en lo anteriormente citado, se buscó responder al objetivo principal de la investigación, mediante la búsqueda de bases y fundamentos de la ciberseguridad, analizar las carencias, debilidades y oportunidades de los programas de estudio en general sobre la carrera de informática, y con base en eso, establecer una solución moderna en la que se pueda satisfacer la demanda de profesionales en dicha área y, por último, orientar con material didáctico certificado al aspirante.

## MÉTODO

Como fase inicial de la investigación, se inició con las cualidades y requerimientos que debía cumplir un informático para poder entender en su totalidad el área de la ciberseguridad. Para estandarizar el esquema de la investigación como tal, se decidió basar toda la investigación como un proyecto orientado a las áreas de conocimiento del PMBOK (producto del Project Management Institute), ya que según el PMI "… se enfoca principalmente en: estándares de desarrollo, investigación, publicación, presentación de seminarios, y ofrecer la guía sobre la gerencia y desarrollo de proyectos…" (Project Management Institute, 2013), y con ello poder concretar un proyecto de la manera más eficaz. También para definir y proponer el resultado de la investigación,

se decidió, hacer un diseño instruccional el cual definiría el proceso de enseñanza de las bases y una introducción a la ciberseguridad.

Como segundo paso en la investigación, se buscó una manera en el cuál se podía no solo clasificar las bases si no también calendarizarlas, se decide optar por la modalidad de un diseño instruccional, que como lo menciona Santaella (2012) sirve para "…desarrollar experiencias de aprendizaje significativas y autorreguladas que produzcan una comprensión duradera en los alumnos…" (Santaella, 2012, pág. 470). Dicho diseño instruccional iba a contener los requerimientos necesarios para el aprendizaje de la ciberseguridad, una fase inicial y una división de temas para poder profundizar en cada tema, además de agregar una práctica de laboratorio por cada una de las lecciones impartidas. Con la búsqueda de cada modelo instruccional se logra dar un enfoque especializado para la facilitación de procesos de aprendizaje de la seguridad informática de manera que el ingeniero interesado en el campo, pueda sacar un mayor provecho y si la materia pueda ser presentada de una manera que no sea tediosa ni repetitiva.

Como objeto de estudio en la investigación, se decidió utilizar dos fuentes confiables para poder tener resultados tangibles. Las dos fuentes satisfacen la problemática general del estudio ya que engloban tanto el aspecto académico como el profesional. Por eso, para satisfacer el ámbito académico se decidió buscar dentro de la Universidad Latina los conocimientos de los estudiantes en comparación al programa de estudio actual de la facultad de Tecnologías de Información de dicha institución. Por el aspecto profesional, se buscó una empresa con una presente demanda y con un departamento de ciberseguridad, con renombre a nivel global como es el IBM (International Business Machines Corporation). Dicho departamento cumple con los requisitos necesarios para buscar opinión experta, recursos didácticos y tecnológicos y experiencia de primera mano. Ambos aspectos fueron necesarios para definir lo que sería el marco teórico e investigativo del proyecto.

Una vez tomada toda la información básica de la ciberseguridad, de manera resumida y concreta, se procede a dar un enfoque metodológico a la investigación, en la cual se planifica como se va a modelar la toma de datos para tener una situación actual y una realidad en Costa Rica sobre el conocimiento básico de esta área de la informática. Se decide centralizar una muestra dentro de la población estudiantil de la carrera de Ingeniería de Sistemas de la Universidad. Con ello se toma

información de tanto el Director de la Carrera, como una encuesta a los estudiantes de la misma. La información obtenida del Director de la Carrera fue fundamental para tener una idea general de cómo está estructurada la carrera actual, qué estándares utiliza y qué tan seguido se actualiza la carrera.

## DESARROLLO

Como punto de partida de la investigación, se establecieron los conceptos de ciberseguridad y la etimología de la palabra "hacker", su filosofía y lo que conlleva. Seguido de eso, se profundiza en aspectos básicos como requerimientos sobre la adquisición de conocimiento de ciberseguridad, las distintas áreas que posee dicha disciplina, herramientas y técnicas. También se busca dar contexto de la ciberseguridad con un poco de historia general acerca de los pioneros y cómo nace esta disciplina.

Otra parte de suma importancia para la investigación, fue dentro del esquema de la seguridad informática, es el saber "de qué es necesario protegerse". El tema de ciberseguridad nace a partir del hecho del robo de datos, ya sea para beneficio personal o el de un tercero según su objetivo como los explica Setfree (2015) en su artículo sobre la clasificación de los tipos de hackers (Setfree, 2015). Desde el nacimiento del internet y almacenamiento de datos en la nube, ha hecho que el interés por adquirir los datos de manera ilícita incremente. La digitalización de los datos ha hecho que las técnicas para robar la información se vuelvan cada vez más sofisticadas. Según la revista Business Insider se dice que "Cisco predice que más de 50 billones de dispositivos van a estar conectados a internet para el 2020" (Danova, 2013). Esto obliga al especialista de ciberseguridad estar al tanto de las últimas tendencias, funcionabilidad de software y la plataforma donde está instalado y lo más importante, los métodos de ataque que se utiliza para robar información. Durante la investigación se determinan no solo los tipos de ataques, sino también la estructura general que conlleva coordinar un ataque a un sistema específico, al igual que las técnicas tanto tecnológicas como sociales, esto se debe a que según el artículo web de Cepeda (2008) "…atacantes externos representan una amenaza mayor en comparación con los ataques internos. Según el estudio, un 73 % involucra ataques externos mientras que un 18 % involucra ataques internos. Normalmente se maneja en la comunidad de seguridad que los atacantes internos

son más peligrosos que los externos" (Cepeda, 2008). Por último, se analiza un poco de historia de cómo nacen estos ataques y cómo son adaptados para poder ser utilizados a favor de un atacante.

Mediante un análisis cuantitativo y cualitativo se busca obtener información dentro de los dos sujetos de investigación. Por el lado profesional, dentro del departamento de Ciberseguridad de IBM, se obtuvo mediante entrevistas tanto a expertos como al personal administrativo, sobre las cualidades y necesidades de un especialista de seguridad informática. También se estableció un contexto sobre cómo se ponen en práctica la teoría en un ambiente ético de trabajo donde se trabaja con información sensible en todo momento. Se enfocó en qué medidas se toman diariamente para proteger la información, que responsabilidades tiene el especialista y los distintos roles que se ejercen dentro del departamento.

Por el lado académico se procedió a dar dos enfoques, el enfoque administrativo y el enfoque estudiantil. Mediante una entrevista al director de la carrera, se obtuvo una perspectiva el conocimiento de ellos de la presente demanda de profesionales y cuáles son sus intenciones con respecto a dicha temática. Por otro lado, en el enfoque estudiantil, se optó por realizar una encuesta sencilla en donde se le cuestiona al estudiante sobre el conocimiento general y ciertas áreas específicas sobre la ciberseguridad. Como la encuesta fue hecha en un formato digital, se aprovechó de una herramienta que cuantifica los datos genera gráficas y provee información pertinente para los resultados de las encuestas sumado a la información obtenida por las entrevistas.

## RESULTADOS

Con respecto a la encuesta, se realizó una serie de preguntas generales en las cuales que ayudaban a identificar el nivel real de una muestra de la población estudiantil. Por motivos de longitud, sólo se van a hacer referencia las preguntas más relevantes de la investigación que fueron determinantes para la obtención de resultados.

En la primera pregunta se pretendía tener un grupo diverso de encuestados en distintos puntos de la carrera de sistemas, como lo muestra la siguiente gráfica.

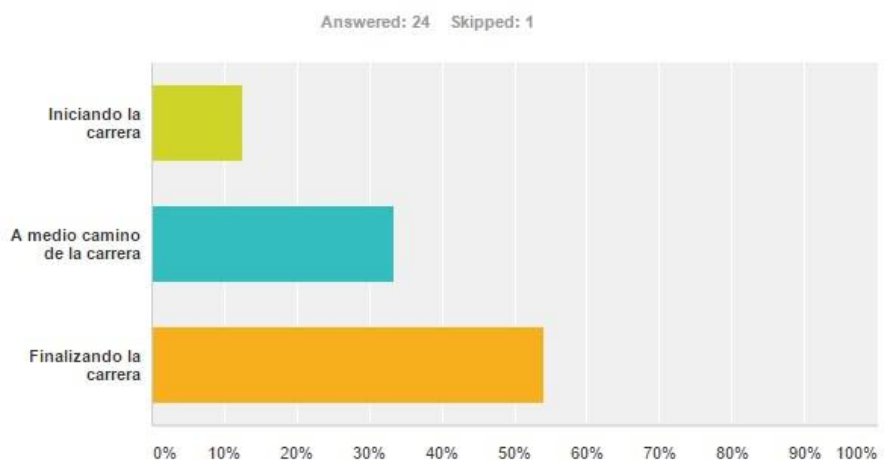


*Ilustración 1.Gráfica de las respuestas para la pregunta 1 de la encuesta. Fuente: (SurveyMonkey, 2015)*

Para la tercera pregunta, se redactaron una serie de estatutos, algunos reales algunos son mitos, y se buscaba que el encuestado pudiera distinguir los reales de los no verdaderos. Las respuestas mostraban un nivel de qué tan de acuerdo estaban con cada uno de los estatutos. La siguiente gráfica de muestra un porcentaje muy similar en cada una de las respuestas, demostrando muy poca consistencia a la hora de responder lo que se les presentaba. Mientras en unas respuestas respondían correctamente, en otras frases similares tenían resultados incorrectos. La siguiente gráfica muestra el porcentaje obtenido por cada pregunta demostrando lo que se explicó anteriormente.

| | Totalmente en desacuerdo | Desacuerdo | No Conozco el término | De Acuerdo | Totalmente de Acuerdo | Total | Weighted Average |
|---|---|---|---|---|---|---|---|
| Un Hacker es un ladrón de información en un sistema informático. | 12.00% 3 | 24.00% 6 | 4.00% 1 | 40.00% 10 | 20.00% 5 | 25 | 3.32 |
| Un Hacker ético provee consultoría sobre seguridad informática a una empresa. | 8.00% 2 | 8.00% 2 | 4.00% 1 | 48.00% 12 | 32.00% 8 | 25 | 3.88 |
| Un Hacker posee un vasto conocimiento de informática, tanto en programación, telemática, bases de datos o sistemas operativos. | 12.00% 3 | 8.00% 2 | 8.00% 2 | 40.00% 10 | 32.00% 8 | 25 | 3.72 |
| La palabra Hacker es un denomitivo para criminal cibernético. | 12.00% 3 | 40.00% 10 | 4.00% 1 | 32.00% 8 | 12.00% 3 | 25 | 2.92 |
| Un Hacker es una persona que ingresa sin permiso a las cuentas personales de un tercero. | 12.00% 3 | 24.00% 6 | 0.00% 0 | 44.00% 11 | 20.00% 5 | 25 | 3.36 |
| La información es el objetivo principal de un Hacker al tratar de penetrar un sistema. | 8.00% 2 | 20.00% 5 | 0.00% 0 | 52.00% 13 | 20.00% 5 | 25 | 3.56 |

*Ilustración 2.Tabla del análisis estadístico de la pregunta 3 de la encuesta. Fuente: (SurveyMonkey, 2015)*

Los resultados obtenidos de la encuesta demuestran varios puntos importantes a considerar. De la población estudiantil, existe un porcentaje muy escaso que posee conocimientos generales de informática. Se puede concluir que mucha de la información que consiguen, no proviene de una institución académica, programa de estudios acreditado o certificaciones de organizaciones reconocidas. El conocimiento es básico, poco estandarizado y se determina junto con la investigación que las entidades académicas ofrecen los programas de estudio orientados a la ciberseguridad en postgrados, especializaciones o certificaciones, lo cual hace que los estudiantes e interesados en el área de la informática se entere de esta área muy tarde en la carrera y oriente su interés a otras áreas las cuales tiene conocimiento desde tempranas etapas de la carrera. Esto tiene un gran impacto a la demanda actual de especialistas en seguridad informática del país, ya que son escasos los profesionales

completamente capacitados para ejercer en dicha área o que posean una educación desde una etapa temprana en su formación.

## DISCUSIÓN Y PROPUESTA

Para mitigar esta faltante de especialistas en seguridad, se propone un diseño instruccional que muestre mediante una taxonomía eficaz, no solo provea a los interesados en el área las bases y la teoría de la ciberseguridad, sino también la aplicación práctica de estos conocimientos mediante actividades, ejercicios y laboratorios. Se opta por utilizar la "Taxonomía de Broudy (1988)" (Santaella, 2012, pág. 472). Esto se debe a que dicho modelo le da un enfoque más comprensivo a la materia, lo cual es esencial a la hora de exponer las bases y fundamentos de un tema, en beneficio de un desarrollo o profundización posterior sobre el tema. Dicha taxonomía engloba el conocimiento mediante el asocie de la materia con un tema específico, en donde el estudiante busque una aplicación práctica y una interpretación para facilitar el conocimiento. De esta manera se le dará al interesado una orientación temprana en la carrera y pueda llevar una progresión en conjunto a las otras áreas de la informática y tener un desarrollo más completo de un profesional en informática. Con dicho diseño instruccional, disminuiría la curva de aprendizaje de la ciberseguridad, y ofrece un proceso de enseñanza estandarizado donde oriente al interesado a una especialización y a programas de estudio reconocidos tanto dentro como fuera de la institución académica.

El diseño instruccional propuesto, engloba un esquema de 15 semanas en el cuál, mediante la taxonomía seleccionada, se busca un enfoque de retroalimentación sobre las lecciones pasadas, y dar un aporte incremental con cada tema abarcado. Para enriquecer cada una de las clases se propone un laboratorio para poner en práctica los conocimientos adquiridos, un objeto de investigación y una discusión general sobre los temas. Esto último para fomentar la investigación individual del aspirante y que pueda enriquecer lo que se está exponiendo en cada clase.

## REFERENCIAS

Cepeda, F. (26 de Junio de 2008). *¿Amenaza interna o externa?* Obtenido de Netmedia Blog: http://www.netmedia.mx/blog/colaboradoresexternos/%C2%BFamenaza-interna-oexterna/

Danova, T. (2 de Octubre de 2013). *Business Insider*. Obtenido de Morgan Stanley: 75 Billion Devices Will Be Connected To The Internet Of Things By 2020: http://www.businessinsider.com/75-billion-devices-will-be-connected-to-theinternet-by-2020-2013-10

Feliu, L. (2013). Seguridad Nacional y Ciberdefensa. Aproximación Conceptual: Ciberseguridad y Ciberdefensa. *Conferencia en la UPM- Escuela Superior de Ingenieros de Telecomunicaciones* (pág. 6). Madrid: Universidad Politécnica de Madrid.

Higgins, K. J. (2008). Hacker's Choice: Top Six Database Attacks. *Dark Reading*, Edicion Web.

Project Management Institute. (2013). *Guía de los Fundamentos para la Dirección de Proyectos.* Newtown Square, Pensilvania: PMI.

Santaella, C. D. (2012). Conocimiento Didáctico General Para El Diseño Y Desarrollo De Experiencias De Aprendizaje Significativas En La Formación Del Profesorado. *Profesorado, Revista de Currículum y Formación del Profesorado*, 470.

Setfree, L. (Noviembre de 2015). *¿Qué es un hacker?* Obtenido de Batanga: http://www.batanga.com/tech/13182/que-es-un-hacker