PAAKAT: revista de tecnología y sociedad
ISSN: 2007-3607
Universidad de Guadalajara, Sistema de Universidad Virtual

Roque Hernández, Ramón Ventura; Juárez Ibarra, Carlos Manuel
Concientización y capacitación para incrementar la seguridad informática en estudiantes universitarios
PAAKAT: revista de tecnología y sociedad, núm. 14, 00005, 2018, Marzo-
Universidad de Guadalajara, Sistema de Universidad Virtual

DOI: https://doi.org/10.18381/Pk.a8n14.318

Disponible en: https://www.redalyc.org/articulo.oa?id=499063347005

Paakat: Revista de Tecnología y Sociedad
e-ISSN: 2007-3607
Universidad de Guadalajara
Sistema de Universidad Virtual
México
suv.paakat@redudg.udg.mx

Año 8, número 14, marzo-agosto 2018

Concientización y capacitación para incrementar la seguridad informática en estudiantes universitarios

Awareness and Training to Increase Cyber-Security in University Students

Ramón Ventura Roque Hernández*
Universidad Autónoma de Tamaulipas, México

Carlos Manuel Juárez Ibarra**
Universidad Autónoma de Tamaulipas, México

[Recibido: 29/12/2017. Aceptado para su publicación: 9/02/2018]
DOI: http://dx.doi.org/10.32870/Pk.a8n14.318

Resumen

Este artículo presenta una investigación realizada para explorar las deficiencias en seguridad informática que poseen los alumnos universitarios de licenciatura en informática en sus primeros semestres, y para evaluar preliminarmente el efecto que tendría un programa de capacitación y concientización diseñado para ellos. Se trabajó con un solo grupo de participantes, a quienes se encuestó antes y después de un evento formativo en modalidad de conferencia. Para analizar los datos se utilizó el software SPSS, donde se realizaron pruebas no paramétricas de Wilcoxon para buscar diferencias entre las respuestas recabadas antes y después del evento. Se encontró que los participantes podrían tener mayores niveles de conocimientos y seguridad en sus actividades cotidianas de cómputo, y que el evento logró incrementar indicadores tales como la percepción de

conocimientos sobre seguridad informática y la conciencia de realizar respaldos más frecuentemente. Los resultados preliminares muestran un efecto positivo que motiva a implementar un programa permanente de concientización y capacitación.

Palabras clave
Educación superior; tecnología de la información; internet.

Abstract

This paper presents a research aimed at: 1) exploring the deficiencies in cyber security that freshman university students of Information Technology (IT) undergraduate programs have, and 2) evaluating the effect that an awareness and training program designed for them would have. In this research, one group of students participated; they were surveyed before and after a training activity that was presented to them as a conference. The responses of the participants were analyzed using the SPSS statistical software, and several Wilcoxon non parametrical tests were performed to find differences before and after the event. It was found that participants could have higher levels of knowledge and safety in their daily activities; also, it was found that the conference increased the perception about cyber-security concepts and the awareness to create information back-ups more often. These preliminary results show a positive effect that encourages to implement a permanent training and awareness program.

Keywords

Higher Education; Information Technology; Internet.

Introducción

La seguridad informática hoy día es un tema central para todos los usuarios de equipos de cómputo, ya sean de escritorio o móviles, en el hogar, en la escuela o dentro de una organización. Esto se debe a que el uso del Internet con su popularización ha traído consigo importantes riesgos de seguridad. El Internet es usado para propósitos para los cuales no fue concebido desde su creación. Inicialmente el Internet fue diseñado para promover la conectividad y no la seguridad (Jenab y Moslehpour, 2016).

La veloz adopción de Internet, dispositivos móviles y aplicaciones en la nube han causado que las compañías no implementen al mismo ritmo medidas que mejoren la seguridad para enfrentar las amenazas del mundo actual (Stanciu y Tinca, 2016). Todos los usuarios de medios informáticos deberían tener un sentido crítico sobre las actividades que realizan en sus computadoras, especialmente conectados por medo de Internet. Sin embargo, aún hoy muchos usuarios parecen relegar la seguridad informática a un segundo plano de interés.

Este artículo presenta una investigación que se realizó con los objetivos de explorar las deficiencias en el área de seguridad informática que poseen los alumnos universitarios de licenciatura en informática en sus primeros semestres, y de evaluar preliminarmente los efectos que tendría un programa de capacitación y concientización orientado a incrementar el nivel de seguridad informática de estos alumnos en sus tareas de cómputo cotidianas. Como diseño de investigación se eligió trabajar con un solo grupo de participantes, a quienes se les encuestó antes y después de un programa formativo en modalidad de conferencia.

El trabajo se encuentra organizado de la siguiente manera: primero se exponen los antecedentes del tema, donde se incluyen las definiciones técnicas utilizadas en este artículo, así como el trabajo previo bajo esta misma línea de investigación. Posteriormente se explica la metodología seguida para este estudio, donde se plasman detalles de los participantes, escenario, instrumento de recolección, intervención, tipo de estudio y diseño de investigación, así como la definición conceptual y operacional de las variables. Después se presentan los resultados obtenidos en el análisis estadístico de los datos y la discusión con sus implicaciones. Finalmente, se abordan las conclusiones del estudio.

Antecedentes

La seguridad informática

La seguridad es un tema que ha ganado cada vez más relevancia para las ciencias de la computación, debido al crecimiento de internet y al volumen de intercambio de datos que se realiza hoy en día (Forouzan, 2003). La seguridad informática no solamente busca proteger a los equipos y datos, sino también a las personas.

Para esto la educación y la concientización deben ser valoradas como herramientas útiles contra incidentes peligrosos. Por ejemplo, a los usuarios se les puede capacitar acerca de medidas preventivas y buenas prácticas que les ayuden a entender en qué consisten las amenazas y como protegerse de ellas. De esta manera los usuarios pueden ser más cautelosos y aumentar el nivel de seguridad que tienen en sus actividades de cómputo diarias.

Dentro de la seguridad informática existen muchos términos y problemas que los usuarios deberían conocer. En nuestro trabajo hemos centrado la atención en los siguientes: *hackers*, *crackers*, gusanos, troyanos, *spyware*, *phishing* y respaldos de información. A continuación, se abordará cada uno de ellos.

Hackers y crackers

De acuerdo con Magazine (2009), un hacker es una persona con alto nivel de conocimientos técnicos que utiliza una computadora para tener acceso a un equipo o red, con el objetivo de realizar actividades no autorizadas. Algunos expertos argumentan que los *hackers* poseen principios éticos y que sus acciones no llevan una intención maliciosa. Por el contrario, un *cracker* aunque hace lo mismo que un hacker sí tiene unos objetivos maliciosos implícitos en su conducta.

Gusanos, troyanos y spyware

El código malicioso es cualquier programa escrito para producir inconveniencias al usuario (Miguel-Pérez, 2015). Sus acciones pueden incluir destrucción de datos, uso indebido de recursos y robo de información. Gusanos, troyanos y *spyware* son ejemplos de este tipo de código.

Jenab y Moslehpour (2016) definen a los gusanos como programas maliciosos que se pueden replicar a sí mismos, y se pueden adquirir en distintos lugares por ejemplo en internet a través de mensajería instantánea, o en redes para compartir archivos. Aunque los gusanos son ampliamente conocidos por los usuarios siguen teniendo éxito en sus infecciones, debido a las vulnerabilidades de seguridad de los sistemas actuales.

Los troyanos son programas que no se replican a sí mismos, sino que ofrecen al usuario una funcionalidad aparentemente útil como la de eliminar virus en su sistema. Una vez que se ejecutan estos programas infectan el equipo con virus que puede enviar información, brindar acceso remoto o deshabilitar opciones de protección. Los troyanos son difíciles de detectar, pues aparentan ser programas útiles, pero son justamente lo opuesto y ralentizan las operaciones de la computadora.

El término *spyware* se refiere a programas que recolectan información de un usuario sin su conocimiento. Estos programas pueden ser usados para mostrar contenidos relevantes para el usuario o bien para instalar otros programas que pueden recabar información de las teclas oprimidas y de esta manera robar contraseñas o registrar el historial de búsquedas. El *spyware* no intenta replicarse a otras computadoras.

Phishing

El *phishing* es una manera de robar información a través de un correo electrónico que parece provenir de una organización legítima (Aston, 2016). El correo incluye un enlace que conduce a un falso sitio, el cual es una copia del original y se encarga de engañar al usuario para robar contraseñas, información personal o de tarjetas de crédito.

Hasta hace algunos años resultaba sencillo identificar este tipo de amenazas, pues contenían elementos que visiblemente resultaban sospechosos. Por ejemplo, su diseño era burdo o su redacción era deficiente. Hoy es más difícil identificar si un correo es legítimo o no, pues la calidad de las falsificaciones se ha incrementado notablemente.

Respaldos de información

La información es un activo importante para empresas y para personas (Rhodes-Ousley, 2013), por lo cual es necesario asegurarla; una manera de hacerlo es a través de respaldos. Un respaldo es una copia de los archivos importantes de un sistema informático que se realiza con la finalidad de prevenir la posible pérdida debido a errores de *hardware*, *software* o infecciones de virus por mencionar algunas causas.

Los respaldos pueden ser completos, es decir, de todos los archivos, o bien incrementales. Solo de los archivos que han cambiado desde el último respaldo; la decisión de realizar un respaldo completo o incremental puede acelerar o alargar considerablemente el proceso de copia de los archivos (Stier, 2015).

Los respaldos deberían realizarse periódicamente y almacenarse en sitios distintos donde radica el equipo de cómputo para prevenir la pérdida por desastre físico. De esta manera, la nube es una buena opción para guardar los respaldos, pues sus servidores se encuentran geográficamente distantes del equipo que está siendo respaldado.

Programas de concientización y entrenamiento

Wiseman (2017) y Peterson (2017) resaltan la importancia de la capacitación a los usuarios, pues sin importar sus buenas intenciones o las nuevas tecnologías que usen, los seres humanos siempre son el eslabón más débil en la cadena de protección a los datos. Wiseman, además, considera que la concientización es clave en la batalla contra los intrusos y aconseja realizar evaluaciones periódicas entre los usuarios para determinar si reconocen vulnerabilidades potenciales, para de esta manera actuar en consecuencia y mejorar la seguridad informática de una organización.

De acuerdo con Rhodes-Ousley (2013), los programas de concientización en seguridad informática son herramientas útiles para educar a los usuarios de medios informáticos acerca de las conductas que se esperan de ellos, de las acciones que deben realizar en determinados escenarios y de las consecuencias de no seguir las reglas establecidas.

Un programa de concientización también es una ayuda para que las personas comprendan la importancia de seguir las reglas y de los beneficios al tomar medidas que ayuden a incrementar la seguridad de sus datos. El objetivo principal de un programa de concientización es cambiar comportamientos, hábitos y actitudes; algunos recursos para lograrlo incluyen seminarios, entrenamientos en línea, vídeos, correos electrónicos, posters y juegos. Este objetivo se debe cumplir a través de un proceso continuo a largo plazo y debe cuidarse de no saturar a los usuarios con demasiada información a la vez.

Algunos temas que se abordan en estos programas son: privacidad de la información, vulnerabilidades de *software* y *hardware*, códigos maliciosos como virus, gusanos, troyanos, *software* espía y los daños que pueden causar. Rhodes-Ousley menciona que un programa de concientización puede fracasar por varias razones, entre las cuales se encuentran la falta de incentivos para motivar la participación de los usuarios, así como la falta de mediciones para asegurarse que los usuarios están entendiendo el material y para evaluar su comportamiento en escenarios predeterminados.

En el trabajo de Peltier (2002) se destaca que un programa efectivo de concientización en seguridad informática permitirá que los usuarios entiendan las razones por las cuales deben tomar en serio la seguridad informática; las ganancias que obtendrán al implementarla y cómo esto les ayudará en sus tareas cotidianas.

Peltier también menciona que un programa de esta naturaleza debe buscar reducir pérdidas asociadas con la divulgación intencional o accidental de información, así como la modificación o destrucción de datos; de esta manera los usuarios mejorarán la eficiencia y la productividad en sus tareas.

Peltier recomienda que las sesiones de capacitación duren menos de cincuenta minutos, y se preparen con vocabulario adecuado a la audiencia para lograr mantener la atención y el interés de los asistentes. Las sesiones se pueden calendarizar durante las actividades regulares de los usuarios, pero cuidando de no interferir con las horas más ocupadas para ellos.

Trabajos previos

De acuerdo con Dunn Cavelty (2014) los enfoques utilizados para brindar seguridad informática parecen no estar funcionando, pues los niveles de seguridad decrecen cada vez más en lugar de incrementarse. Esto es debido a que la seguridad es un fenómeno multidimensional, el cual frecuentemente se concibe como un aspecto técnico y separado de los elementos humanos de la computación. La concientización acerca de los requerimientos de seguridad podría ayudar a obtener mejores resultados.

North y Pascoe (2016) indican que la ciber-seguridad es un tema de creciente preocupación, especialmente para las empresas del sector privado, pues son ellas las cuales con mayor frecuencia son víctimas de costosos ataques informáticos. En su trabajo ellos resaltan la importancia de concebir la seguridad como un tema de interés para toda la organización, y no solo para el departamento de tecnología.

En este proceso los directivos tienen una tarea muy importante, pues deberían proveer los medios necesarios para promover una continua cultura de concientización sobre la seguridad informática. Además, deben asegurarse que existan los recursos económicos para que pueda ser implementado un programa permanente el cual apoye esta cultura entre todo el personal.

En las universidades la concientización tiene un rol importante para crear entre los estudiantes una percepción aguda sobre los riesgos de seguridad informática. Ellos son futuros profesionistas que pronto deberán hacer frente a las amenazas informáticas como parte de su vida profesional. Existen investigaciones que han identificado la importancia que la seguridad sea fomentada e investigada desde el ámbito universitario.

El trabajo de Stanciu y Tinca (2016) resalta la necesidad urgente de implementar programas de capacitación y concientización acerca de la seguridad informática, especialmente en las universidades, pues el conocimiento de los estudiantes suele ser más técnico y específico de su campo de estudio y menos orientado hacia aspectos de seguridad. Se destaca que la actitud de las personas, aunada a su conducta, representa una debilidad muy importante. Por ejemplo, los errores humanos cometidos sin intención y el mal uso de los sistemas por parte del personal han ocasionado graves incidentes de seguridad.

En el trabajo de Kiani (2016) se estudia la percepción sobre la seguridad informática que tienen los alumnos de una universidad, la cual ofrece programas académicos en línea; se aborda la influencia de las características individuales como edad, sexo y estado civil, así como aspectos de la confianza social sobre la percepción de la seguridad informática. En ese trabajo se encontró que a mayor confianza social la percepción de la seguridad informática aumenta, mientras que a mayor edad de las personas la percepción de seguridad disminuye.

En la investigación de Case y King (2013) se realizó un estudio longitudinal sobre percepciones y hábitos relativos a la seguridad informática en estudiantes de licenciatura. Se encontró que el número de correos electrónicos con *spam* y *phishing* que habían recibido los alumnos ha disminuido en los últimos años; también decreció su nivel de preocupación sobre ataques y robo de identidad.

Por otra parte, se encontró que los alumnos en esa universidad reportaron una conducta informática más segura en los últimos años que al principio de la investigación. Este cambio positivo en sus hábitos se atribuye a la capacitación proactiva acerca de seguridad que los alumnos han estado recibiendo en sus clases regulares.

Whitty, Doodson, Creese y Hodges (2015) estudiaron específicamente las malas prácticas de las personas en relación con las contraseñas. Ellos encontraron que las personas conocen las recomendaciones para el uso adecuado de contraseñas; sin embargo, se muestran optimistas al creer que es improbable que a ellos les ocurran incidentes negativos, por tanto, no valoran las consecuencias negativas de sus malas prácticas.

También encontraron que la gente joven es más proclive a compartir sus contraseñas con otras personas, y que los programas educativos sobre seguridad deberían incluir a las personas jóvenes como objetivo principal. En este contexto se subraya también que el conocimiento no es suficiente para cambiar las conductas peligrosas relacionadas con la ciber-seguridad, y se muestra evidencia que la capacitación debería promover también la concientización y no solo el conocimiento técnico si en realidad se desean eliminar las malas prácticas.

Metodología

Participantes

Los participantes de esta investigación fueron seis alumnos de segundo semestre de la Licenciatura en informática (LI) de la Facultad de Comercio, Administración y Ciencias Sociales (FCACS) de la Universidad Autónoma de Tamaulipas (UAT), en Nuevo Laredo. El estudio se realizó en el periodo de clases de primavera del año 2017, donde había 27 alumnos registrados en el segundo semestre de LI en la FCACS.

Aunque todos estuvieron presentes en algún momento del evento de capacitación se desestimaron las respuestas de once participantes, porque los alumnos no respondieron el cuestionario en alguno de los dos momentos en que se realizaron las mediciones. Esto ocurrió porque llegaron tarde, se retiraron antes de terminar el evento o salieron por algunos instantes.

Escenario

Este estudio se realizó durante un evento de capacitación en ciber-seguridad, el cual duró cincuenta minutos y estuvo dirigido a los estudiantes de LI de la FCACS. El evento se llevó a cabo en las instalaciones de un centro de cómputo ubicado dentro de la misma facultad, y fue calendarizado durante el horario regular de clase de los alumnos, pero de manera separada a las materias que ellos cursaban en ese semestre.

Los profesores propusieron esta capacitación, atendiendo a las deficiencias que habían observado en los alumnos de los primeros semestres sobre el tema de seguridad informática. De no haberlo hecho se habrían ignorado severos riesgos para los alumnos y para los recursos de cómputo en la universidad que ellos usan regularmente. Los temas propuestos para la capacitación incluían: vulnerabilidades, virus, gusanos, troyanos, *spyware*, *phishing*, medios de prevención, diagnóstico y recuperación de eventualidades, así como también los conceptos de *firewall*, *hackers* y *crackers*.

Estos contenidos fueron impartidos de manera gratuita por un experto profesional externo a la universidad. El expositor estudió la licenciatura en informática y una maestría en tecnología informática. Además de tener experiencia docente resulta propietario de un

negocio dedicado al desarrollo de *software* y al soporte técnico, el cual cuenta con un número importante de clientes en la localidad.

Los estudiantes tuvieron la oportunidad de escuchar la exposición sobre los temas con un enfoque ameno, práctico y aplicado. También pudieron interactuar haciendo preguntas y comentarios al expositor. En la sala se contó con suficientes asientos para los asistentes, clima artificial y un vídeo proyector para mostrar una presentación electrónica.

Instrumento

Para la recolección de datos se utilizó el cuestionario que se muestra en la tabla 1. Se solicitó responder las preguntas P1 a P5, utilizando una escala de 0 al 10. El cero representaba: "absolutamente ninguno/nada" y diez "mucho". La pregunta 6 se presentó con las siguientes posibles respuestas con sus codificaciones numéricas indicadas entre paréntesis: hoy (0), mañana (1), en esta semana (2), en dos semanas (3), en tres semanas (4), en un mes (5), en más de un mes (6).

En esta pregunta, entre más grande fuera el valor numérico en la respuesta, la fecha para que el alumno realizara su siguiente respaldo también era más lejana. Es importante destacar que la versión del cuestionario que se muestra en la tabla 1 es el resultado de un par de refinamientos que consistieron en la valoración de expertos y en la aplicación de una prueba piloto; estos procedimientos permitieron ajustar la redacción y el orden de las preguntas, así como las escalas de las respuestas.

Tabla 1. Preguntas realizadas a los estudiantes

Identificador	Pregunta
P1	¿Qué nivel de seguridad tienes en tus actividades de cómputo diarias?
P2	¿Qué nivel de conocimientos tienes sobre seguridad?
P3	¿Qué tan claras tienes las diferencias entre *hacker* y *cracker*?
P4	¿Qué tan claras tienes las diferencias entre gusano, troyano y *spyware*?
P5	¿Qué tanto sabes de *phishing*?
P6	¿Cuándo será el siguiente respaldo de tu información?

Fuente: elaboración propia.

Intervención

Primero los estudiantes fueron encuestados momentos antes de la capacitación. Posterior se llevó a cabo el desarrollo de los temas por parte del experto invitado e inmediatamente después se volvió a encuestar a los mismos alumnos con el objetivo de conocer el efecto de la capacitación que se les ofreció. En ambos momentos los cuestionarios fueron entregados a los alumnos en hojas blancas tamaño media carta con las preguntas y posibles respuestas impresas. Los participantes marcaron sus respuestas, utilizando los bolígrafos que se les facilitaron.

Tipo de estudio y diseño de investigación

Se hizo un estudio experimental de un solo grupo con pre-test y post-test. Con este diseño de investigación es posible realizar una comparación de los mismos individuos antes y después de un tratamiento. La diferencia observada en ambos momentos es la medida de la influencia del tratamiento experimental (Zikmund, Barry, Carr y Griffin, 2013).

Definición conceptual y operacional de variables

En la tabla 2 se muestran las variables estudiadas en esta investigación, así como sus definiciones conceptuales y las preguntas asociadas en el cuestionario utilizado:

Tabla 2. Definición conceptual y operacional de variables

Variable	Definición conceptual	Definición operacional y pregunta
Seguridad aplicada	Percepción del estudiante sobre el nivel de seguridad informática que aplica en sus tareas cotidianas	P1
Conocimientos sobre seguridad	Percepción del estudiante sobre el nivel de conocimientos de seguridad que posee	P2
Conocimiento sobre atacantes	Percepción del estudiante sobre el nivel con el que puede diferenciar a un *hacker* y a un *cracker*	P3
Conocimiento sobre amenazas de *software*	Percepción del estudiante sobre el nivel con el que puede diferenciar a un gusano, un troyano o un programa de *spyware*	P4
Conocimiento sobre *phishing*	Percepción del estudiante sobre el nivel de conocimientos que tiene acerca del *phishing*	P5
Tiempo para realizar respaldos de información	Tiempo en el cual el alumno piensa realizar su próximo respaldo de información	P6

Fuente: elaboración propia.

Análisis de datos

Una vez recolectadas las respuestas de los alumnos, antes y después de la conferencia, estas se organizaron y se capturaron utilizando el software SPSS versión 22 (Wagner, 2014). Al utilizar este paquete estadístico se obtuvieron los valores descriptivos para los datos y se condujeron pruebas no paramétricas de Wilcoxon (Anderson, Sweeney y Williams, 2011).

Para cada una de las preguntas de la tabla 1 se advirtió el objetivo de encontrar diferencias estadísticas significativas entre las percepciones de los estudiantes en los dos momentos del estudio. Se utilizó un nivel de confianza de referencia de 95%. De esta manera cualquier PValor (significancia) bilateral menor a .05 en las pruebas de hipótesis

se interpretó como un indicador de la existencia de las diferencias entre las percepciones de los estudiantes antes y después de la conferencia.

Resultados

Las respuestas obtenidas en la aplicación del cuestionario antes de la conferencia se muestran en la tabla 3. El resumen de las respuestas proporcionadas por los estudiantes después de la conferencia se encuentra en la tabla 4. El resultado de la prueba no paramétrica de Wilcoxon se presenta en la tabla 5.

Tabla 3. Datos descriptivos de las respuestas a las preguntas antes de la conferencia

	P1	**P2**	**P3**	**P4**	**P5**	**P6**
Media	6.25	6.63	4.50	5.75	2.31	3.44
Desv. est.	2.463	1.360	2.449	2.769	2.869	2.529
Mediana	7.00	7.00	5.00	6.00	.50	4.00
Rango intercuartil	3	2	5	5	5	5

Fuente: elaboración propia.

Tabla 4. Datos descriptivos de las respuestas a las preguntas después de la conferencia

	P1	**P2**	**P3**	**P4**	**P5**	**P6**
Media	7.00	8.06	9.25	8.63	7.75	1.75
Desv. est.	2.129	1.389	.931	1.544	2.380	1.390
Mediana	8.00	8.50	9.50	9.00	8.00	3.00
Rango intercuartil	4	2	1	2	3	4

Fuente: elaboración propia.

Tabla 5. Resultados de la Prueba no paramétrica de Wilcoxon para buscar diferencias entre las respuestas antes y después de la conferencia

	P1	**P2**	**P3**	**P4**	**P5**	**P6**
Z	-1.170	-3.096	-3.529	-3.022	-3.433	-2.547
PValor bilateral	.242	.002	.000	.003	.001	.011

Fuente: elaboración propia.

Discusión

Discusión de los resultados de las pruebas estadísticas

Al realizar la prueba no paramétrica de Wilcoxon no se encontraron diferencias estadísticas significativas en la pregunta 1, lo cual era esperado, pues se refiere a las prácticas actuales en las actividades diarias de cómputo, las cuales no se modificarían inmediatamente después de una sesión de capacitación, sino hasta pasado algún tiempo.

En la pregunta 2 (¿qué nivel de conocimientos tienes sobre seguridad?) sí se encontraron diferencias estadísticas significativas, siendo la puntuación mayor después de la conferencia. Esto indica que los estudiantes percibieron que sus conocimientos aumentaron con el contenido que se abordó en el seminario.

También se establecieron diferencias estadísticas significativas en la pregunta 3 (¿qué tan claras tienes las diferencias entre *hacker* y *cracker*?), la pregunta 4 (¿qué tan claras tienes las diferencias entre gusano, troyano y *spyware*?) y la pregunta 5 (¿qué tanto sabes de *phishing*?). Estas preguntas hacían referencia a conceptos que se expusieron directamente durante la capacitación; por esta razón es comprensible que las puntuaciones mayores se hayan registrado después de esta.

Llama la atención que los estudiantes en su mayoría reportaron saber poco acerca del término *phishing* antes del evento al que asistieron. Estos hallazgos concuerdan con los de Stanciu y Tinca (2016), quienes en su investigación encontraron que los alumnos desconocen el *phishing* y sus consecuencias a pesar de que este tipo de ataques se incrementa cada vez más.

En la pregunta 6 (¿cuándo será el siguiente respaldo de tu información?) también existieron diferencias entre las respuestas de los estudiantes. Es destacable que antes de la conferencia los alumnos tenían pensado realizar un respaldo de su información en un plazo mayor de tiempo, pero inmediatamente después de la conferencia los alumnos modificaron esta percepción y dijeron que su próximo respaldo lo harían en una fecha más cercana.

Discusión de la implicación de los resultados

Con los resultados obtenidos se observó que los participantes, a pesar de ser estudiantes de la carrera profesional de licenciatura en informática, podrían tener un mayor nivel de seguridad en sus actividades cotidianas de cómputo. Esto tiene especial importancia en una época en la cual las redes e internet se utilizan con mucha frecuencia y la conectividad que ofrecen trae consigo amenazas latentes que los usuarios deben conocer para poder protegerse adecuadamente.

Se observó que el evento de capacitación incrementó la percepción de los estudiantes acerca de sus conocimientos en seguridad informática, y también los concientizó para tomar medidas inmediatas para proteger sus datos. Esto lo interpretamos como un efecto positivo que debe fortalecerse constantemente con actividades orientadas a mejorar la seguridad de los alumnos y de su información.

Si bien es cierto que nuestro trabajo expone la necesidad de contar con programas de capacitación y concientización sobre seguridad informática en las universidades deja al

descubierto los beneficios de la existencia de este tipo de recursos; se deben tener en cuenta las limitaciones de nuestro estudio.

Al ser una evaluación preliminar, en esta investigación centramos nuestra atención en las percepciones de los estudiantes y no realizamos mediciones de sus conocimientos; tampoco evaluamos el efecto del evento de capacitación después de algún tiempo, ambas actividades quedan propuestas para la continuación de este trabajo.

De la misma manera que Wiseman (2017), Peterson (2017) y Rhodes-Ousley (2013) consideramos que la capacitación y la concientización son importantes como medios de prevención y como agentes de cambio en las conductas, hábitos y actitudes de los estudiantes. Recomendamos que estas acciones de capacitación sean para todas las áreas y no solo para los alumnos de carreras profesionales en tecnologías; de esta manera coincidimos con North y Pascoe (2016). Finalmente, ponemos en relieve la necesidad que estas acciones no sean aisladas, sino que enriquezcan los estudios universitarios a través de programas permanentes que aborden las múltiples dimensiones de la seguridad informática.

Conclusiones

En este artículo se presentaron los resultados de un estudio en el cual se destacó la importancia de la concientización y la capacitación en temas de seguridad informática. Se encontró que los conocimientos de los estudiantes de los primeros semestres de una carrera profesional en informática podrían incrementarse para su propio beneficio, y se observó que un evento de capacitación tuvo un efecto positivo en los participantes.

Concluimos que la implementación de un programa permanente con los objetivos de capacitar y concientizar a los estudiantes universitarios acerca de temas de seguridad informática sería benéfico para crear comunidades más seguras con usuarios más protegidos y con mayor conciencia de sus acciones.

Referencias

Anderson, Sweeney y Williams (2011). *Estadística para negocios y economía.* México, México: Cengage Learning.

Aston, G. (2016). Who is phishing for your data? *Trustee,* 69 (2), 8-11.

Case, C. J. and King, D. L. (2013). Cyber Security: A Longitudinal Examination of Undergraduate Behavior and Perceptions. *American Society of Business Behavioral Sciences eJournal,* 9 (1), 21-29.

Dunn Cavelty, M. (2014). Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities. *Science and Engineering Ethics*, 20 (3), 701-715.

Forouzan, B. A. (2003). *Introducción a la ciencia de la computación.* México: Thomson.

Jenab, K. and Moslehpour, S. (2016). Cyber Security Management: A Review. *Business Management Dynamics*, 5 (11), 16-39.

Kiani, M. (2016). Internet Security Feeling of Students. Study of Payame Noor University. *Trakia Journal of Sciences*, 14 (3), 230-235.

Magazine, A. (2009). Unveiling the misterious world of an ethical hacker. *SiliconIndia*, 36-37.

Miguel-Pérez, J. C. (2015). *Protección de datos y seguridad de la información.* México: Ra-Ma.

North, J. and Pascoe, R. (2016). Cyber security and resilence - it's all about governance. *Governance Directions*, 68 (3), 146-151.

Peltier, T. R. (2002). *Information Security, Policies, Procedures and Standards: Guidelines for Effective Information Security Management.* USA: CRC Press LLC.

Peterson, A. (2017). One negligent employee: Ensure security training raises employees' awareness of threats. *Credit Union Magazine*, 10.

Rhodes-Ousley, M. (2013). *Information Security - The Complete Reference.* USA: McGraw-Hill.

Stanciu, V. and Tinca, A. (2016). Students' awareness on information security between own perception and reality - an empirical study. *Accounting and Management Information Systems*, 15 (1), 112-130.

Stier, K. (2015). Data backup in the age of the cloud. *University Business*, 49-51.

Wagner, W. (2014). *Using IBM SPSS Statistics for Research Methods and Social Science Statistics.* USA: SAGE Publications.

Whitty, M., Doodson, J., Creese, S. and Hodges, D. (2015). Individual Differences un Cyber Security Behaviors: An Examination of Who is Sharing Passwords. *CyberPsychology, Behavior, and Social Networking*, 18 (1), 3-7.

Wiseman, C. (2017). Accounting Firm Cybersecurity: Training Your Staff and Protecting Your Business. *CPA Practice Advisor*, 27.

Zikmund, W., Barry, B., Carr, J. and Griffin, M. (2013). *Business Research Methods.* Mason, Ohio, USA: Cengage Learning.

* Ramón Ventura Roque Hernández es ingeniero en Sistemas Computacionales, maestro en Ciencias en Ingeniería Electrónica, doctor en Ingeniería Telemática y doctor en Educación. Actualmente es profesor investigador en la Universidad Autónoma de Tamaulipas, México. Sus intereses de investigación incluyen la ingeniería de software, la informática aplicada y la tecnología educativa.

** Carlos Manuel Juárez Ibarra es licenciado en Informática y maestro en Comunicación Académica. Actualmente es docente de la Universidad Autónoma de Tamaulipas, México, y desarrollador profesional de sitios web. Sus intereses de investigación incluyen la seguridad informática, la tecnología educativa y el desarrollo de software.