ESTRATEGIAS DE PROTECCIÓN EN INTERNET Y LA EDUCACIÓN A DISTANCIA. CASO: POSGRADO EN LÍNEA DE LA UAZ

Hernández Berumen, José de Jesús, Valadez Estrada Raúl Armando y Cordero Dávila, Susana. (2017). Estrategia de protección en internet y la educación a distancia. Caso: Posgrado en línea de la UAZ. Revista Digital FILHA. [en línea]. Diciembre. Número 17. Publicación bianual. Zacatecas: Universidad Autónoma de Zacatecas. Disponible en: www.filha.com.mx. ISSN: 1870-5553.

Resumen: *La presente investigación tiene como propósito general demostrar que los estudiantes de la modalidad en línea del posgrado de la Maestría en Tecnología Informática Educativa perteneciente a la unidad académica de Docencia Superior de la Universidad Autónoma de Zacatecas, carecen de estrategias de protección informática, en especial quienes pertenecen al sexo femenino, utilizan sistema operativo de la familia de Microsoft Windows y no tienen antecedentes académicos en relación a la informática, son los más vulnerables a cierto tipo de ataques informáticos. Para ello se aplicó un instrumento de tipo encuesta validado con Alpha de Cronbach, diseñado acorde a la operacionalización de las variables que definen los objetivos e hipótesis de esta investigación y que utiliza reactivos del tipo de pregunta cerrada, con escalas Likert, recabándose la información de manera digital por medio de Google Forms, aplicado a 106 alumnos del semestre agosto – enero de 2016, de los cuales 42 eran de primer semestre, 23 de segundo, 21 de tercero y 20 de cuarto, su distribución de sexo por cohorte generacional fue 52% sexo femenino y el restante 48% del masculino, posteriormente a la recopilación de datos se realizó un análisis exploratorio y descriptivo de frecuencias y análisis multivariado, con el método factorial de análisis de componentes principales. Los resultados que arrojó esta investigación confirman que la hipótesis establecida es válida. Se concluye que se debe dar instrucción dirigida a estudiantes y facilitadores con el propósito de que adviertan los principales riesgos del uso de la Internet y tengan mejores hábitos de protección.*

Palabras clave: *seguridad informática, educación en línea, posgrado.*

Abstract: *The present investigation has as a general purpose to demonstrate that students of the online graduate program: Educational Information Technology of the Autonomous University of Zacatecas, lack of strategies of computer protection especially those who belong to the female sex. They latter use operating systems of the family Microsoft Windows and they do not have academic antecedents related to the computer sciences, they are the most vulnerable againts certain type of computer attacks. To this end, a survey instrument validated with Alpha de Cronbach was applied, designed according to the operationalization of the variables that define the objectives and hypotheses of this research and which uses reagents of the closed question type, with Likert scales, gathering information from digitally through Google Forms, applied to 106 students of the semester August - January 2016, of which 42 were first semester, 23 were in second semester, 21 were in third semester and 20 were in fourth semester. In this group 52% were female and 48% were male, subsequent to the data collection an exploratory and descriptive analysis of frequencies and multivariate analysis was carried out, using the factorial method of the principal components analisys (PCA). The results of this research confirms hypothesis established as valid. It concluded that instruction should be given to students and facilitators in order to identify the main threats that they face in Internet and enhace their own protection habits.*

Keywords: *informatic security, e-learning, graduate students.*

Introducción

En la actualidad toda interacción en línea por parte de los usuarios mediante las TIC conlleva riesgos adicionales a las ventajas inherentes de su uso (Espinar Ruiz & López Fernández, 2009), y es claro que estas tecnologías han rebasado por mucho las capacidades en cuanto a su correcto empleo por parte de sus usuarios y los posibles riesgos a los que se exponen con ella, cada vez que aparece un sitio, programa o servicio nuevo en la Internet, se suele adoptar casi de inmediato sin cuestionamiento alguno, si es útil de alguna manera y la mayoría de las veces sin una instrucción formal se comienza a utilizar, si surgen problemas en su uso se suele preguntar a alguna persona que se crea utiliza dicha tecnología o que sea instruida en el tema o bien se recurre a la misma Internet para tratar de encontrar la solución al predicamento en distintas fuentes de información como los foros, videos de youtubers, tutoriales, sitios oficiales, etc. con los cuales se podrá documentar el

mismo usuario, sin embargo, todas estas fuentes que se pueden encontrar en la Internet rara vez advierten o educan de una manera correcta acerca de los riesgos en su uso y los estudiantes en posgrados en línea no son la excepción, a final de cuentas son usuarios de las TIC, a pesar de ello, los estudiantes perciben o están enterados de alguna manera de dichas amenazas (Staksrud et al., 2012), y por otro lado, por el simple hecho de ser humanos desde épocas remotas ha existido preocupación por la seguridad en diferentes niveles lo cual es algo no exclusivo de nuestros días (Velasco Melo, 2008).

Los estudiantes que cursan el programa de posgrado de la Maestría en Tecnología Informática Educativa (MTIE) se presentan con problemas que coinciden con las características mencionadas anteriormente y por lo tanto con problemas relacionados a la seguridad informática, por ende, muchas veces solicitan asesoría a los facilitadores para que les ayuden a resolver su problemática informática, razón por la cual algunos alumnos no entregan tareas, bajo los argumentos tales como: que perdieron archivos "accidentalmente" o "misteriosamente", que tuvieron que formatear sus equipos y reinstalar todos los programas que emplean, que adquirieron un virus informático o alguna otra variedad de Malware, que sus equipos están demasiado lentos y no pueden hacer nada o simplemente no arrancan o no funcionan correctamente, o bien, que algún software pirata que utilizan dejó de funcionar, entre muchos otros que incluso no afectan el desarrollo de sus actividades del programa de maestría, pero que sí les afecta en su vida diaria como usuarios de las TIC. Cabe resaltar que la mayor incidencia de problemas se presenta en el género femenino, así como en aquellos que no cuentan con un perfil de estudios con afinidad a las áreas de las TIC y en ambas situaciones se utilizan sistemas operativos de Microsoft. No existe evidencia documental de esto último en bitácoras o estadísticas. Lo único que se recoge es la experiencia de ser el administrador de plataforma y tener que lidiar con el soporte técnico a los alumnos ya que se carece de un staff de apoyo que realice dicha actividad.

Esta realidad como se menciona anteriormente, alerta acerca de que realmente algo está pasando en cuanto a los conocimientos de los estudiantes del programa al respecto de la seguridad informática, lo que los deja vulnerables en cuanto a su derecho universal de la privacidad de información que en el año del 2013 la Asamblea General de la ONU aprobó en su resolución 68/167 que presentó Brasil y Alemania como el ***Derecho de la privacidad en la era digital*** (Organización de las Naciones Unidas, 2015).

De los antecedentes surge el problema de investigación, el cual se define como: ***"El bajo nivel de conocimientos de seguridad informática en los alumnos de posgrado en línea de la MTIE para el uso de la Internet, está determinado por el género, la afinidad informática y el tipo de sistema operativo utilizado"***. Y la hipótesis de investigación a comprobar en este estudio es que: "***Los estudiantes del posgrado de la maestría en tecnología informática educativa que no tienen afinidad informática, que son de sexo femenino y utilizan MS Windows, tienen menos posibilidades de seguridad en Internet".***

Marco Teórico

En este apartado categorizaremos los aspectos principales que afectan la seguridad de los estudiantes como usuarios de las TIC, para ello retomaremos el estudio hecho por Staksrud *et al* (2012) que realizaron a jóvenes y adolescentes en torno a los posibles riesgos asociados al uso de las tecnologías, en el cual encontraron que los temas tratados con mayor frecuencia por parte de los objetos de estudio resultaron ser el contacto con desconocidos, los contenidos inapropiados, las amenazas a su privacidad y lo relacionado al comercio electrónico.

Con los resultados del estudio mencionado, podemos establecer algunos factores que afectan la seguridad a la privacidad de información de los estudiantes en conjunto con otros fundamentales, que son la base de los ataques informáticos que se desarrollan hoy día, y estos son:

- *Compartir información* – Todo lo que los usuarios comparten de manera consciente o inconsciente en los diferentes espacios de la web, que puede ser utilizado en su contra de alguna manera.
- *Contraseñas* – Todo lo referente a los hábitos y manejo de las mismas que pueden afectar los espacios protegidos por el usuario.
- *Descargas de fuentes desconocidas* – De qué manera pueden vulnerar nuestra seguridad informática las descargas de archivos de terceros.
- Intervención de conexiones – Los peligros a los que se exponen los usuarios al navegar en Internet en sus propias conexiones o en redes de terceros.
- *Estrategias de seguridad de los usuarios/estudiantes (hábitos de prevención)* - De qué manera influyen los hábitos o estrategias de protección que emplean los usuarios para protegerse de amenazas informáticas.
- *Sistemas operativos* – El tipo de sistema operativo que se utiliza determina en gran medida el nivel de vulnerabilidad y el número de amenazas al que se enfrentarán los usuarios.

Ahora que se ha establecido el escenario general sobre el cual actúan los tipos malos especialistas para penetrar la seguridad y algunas de las condicionantes que se deben cumplir, no todo es un vasto y desolado paraje de inseguridad informática para los usuarios de las TIC. Los equipos que se adquieren por lo regular traen consigo instalado algún tipo de sistema operativo y algún esquema de protección integrado, que muchas veces lo provee dicho sistema o en su defecto puede venir como una versión “gratuita” o de “periodo de evaluación”, delimitado por una licencia que dura algunos meses o un año regularmente, para que el propietario del equipo decida si renueva la licencia al terminar el periodo evaluativo, esto es esencial en sistemas operativos de Microsoft, pues en otros sistemas como el MacOS, Linux, UNIX, o similares, no parece ser necesario, sin embargo, no son invulnerables.

A pesar de estar protegidos por algún tipo de software anti-Malware, otro mecanismo de protección adicional que eligen los usuarios para disminuir las brechas inseguras que posiblemente dejan expuestas las vacunas o algunos anti-Malwares es la pared cortafuegos o *Firewall* (Davis, Bodmer, & LeMasters, 2009) el cual está diseñado para controlar el tráfico de red que entra y sale de sus equipos, y a su vez permite o denega las conexiones de acuerdo a ciertas políticas de seguridad establecidas por defecto, o bien, creadas por el usuario mismo, esto no es garantía de invulnerabilidad, pero sin duda hace que las intrusiones a sus equipos o redes sean más difíciles, usuarios con mayor nivel de conocimiento en cuanto a seguridad informática, tienden a crear sus propias políticas de conexiones dentro del *firewall*, lo que les brinda un mejor nivel de seguridad y confianza en sus equipos.

Toda esta revolución digital “maravillosa” que ahora abrazan quienes pertenecen a la sociedad de la información, siempre ha presentado riesgos y amenazas. Desde sus inicios despertó la curiosidad en muchas de las personas que tenían acceso a dichas tecnologías emergentes de comunicación, con ella comenzaron a experimentar con fines de aprendizaje o para sacar algún beneficio personal, de aquí se puede empezar a discernir dos tipos de perfiles, los que experimentan con la tecnología sin fines de ofensa a terceros, solo por el placer de buscar fallas en sistemas y comprender como funcionan para expandir su propio conocimiento, por otro lado, quienes buscan el provecho personal y realizan intrusiones nocivas, de invasión o destructivas. Sin embargo, siempre se han confundido estos dos tipos de “expertos”. De acuerdo a Young Susan & Aitel Dave, (2004) aún persiste el debate acerca de la terminología correcta para describirlos, y cita a Bob Woods (1996) el cual escribió un editorial en dicho año cuestionando por qué los medios noticieros utilizan la palabra Hacker a pesar que mucha gente les enviaban correcciones cada vez que hacían esto, el sumario de dicho editorial es: “El público los conoce como hackers – Sabemos que la manera correcta de referirnos a ellos es como Crackers”. Se puede decir que los medios de comunicación han tergiversado el significado de

la palabra “Hacker” que en realidad se ha referido siempre para describir alguien que siempre ha disfrutado aprender detalles de los lenguajes de programación, sistemas de cómputo o algoritmos computacionales, que prefiere codificar (escribir programas) en lugar de planearlos y diseñarlos. Se les conoce también por su pericia como expertos en tópicos específicos, pero la mera definición es más compleja que eso, pues en el auge de la cultura hacker, a finales de los años 80, donde en pizarras de boletines “piratas” que corrían bajo sistemas operativos MS-DOS y bajo la jerga de “skateboarders”, se diferenciaban los diferentes tipos de hackers.

De a cuerdo a Barrón (2004) la educación en línea por parte de instituciones de educación superior en México, inicia de manera formal a finales del año de 2003, donde la Benemérita Universidad de Puebla, el Consejo Británico de México, Escuela Bancaria y Comercial, el Instituto Nacional Indigenista, el Instituto Tecnológico de Estudios Superiores de Monterrey, la Universidad Anáhuac, la Universidad Autónoma de Américas, la Universidad de Monterrey, la Universidad del Valle de México, la Universidad Iberoamericana, la Universidad Juárez Autónoma de Tabasco, la Universidad Nacional Autónoma de México, la Universidad Regiomontana, por resaltar algunas, iniciaron la oferta de cursos, diplomados, especializaciones, e inclusive grados de maestrías, en algunas de ellas.

Nada de eso pudo ser posible hasta esos años, pues hasta el año de 1987 es cuando por primera vez en junio se tuvo una conexión permanentemente en una institución educativa, el ITESM, seguido de la UNAM ese mismo año en octubre, con un acceso a la red BITnet.

La educación a distancia ha sufrido grandes cambios desde sus inicios, en los que la interacción y la comunicación entre el docente y el alumno era empleando medios impresos, de radio y televisión, posteriormente al avanzar la tecnología se incorporaron los casetes de audio y los de video adicionales al fax, al momento que emergen las TIC se revoluciona por completo este modelo y emerge la educación en línea o e-learning (Robles Peñaloza, 2004).

Los estudiantes tienen a su alcance una gran variedad de software a su alcance para su protección: paredes cortafuegos, anti-Malware, herramientas para navegadores como los bloqueadores de ventanas emergentes y filtros phishing (sitios y correos falsos) y anti Malvertising, (Mensch & Wilkie, 2011) sistemas operativos más seguros, entre otros, ¿Qué garantía se tiene de que los estudiantes saben si tienen o no algún tipo de anti-Malware instalado en sus equipos como las vacunas?, o que saben remover un virus una vez que lo descubren, o si están en un sitio falso, o que el certificado de seguridad al sitio que se conectan es válido, la lista de interrogantes puede seguir creciendo.

De acuerdo a White, Hewitt & Kruck (2013) la educación es la mejor contramedida para cuestiones de seguridad informática y de otra índole, dado el sustancial número de incidentes en seguridad en las organizaciones, existe una necesidad por una mayor educación en el área de la seguridad informática, en específico.

Metodología

Esta investigación se realizó bajo el enfoque **cuantitativo**, ya que el interés principal de ésta se situá en explicar, predecir y controlar una realidad; reduce su ámbito de estudio a fenómenos observables susceptibles de medición, así mismo prioriza los análisis de causa-efecto y correlación estadística, utiliza técnicas estadísticas para definir las muestras, análisis de datos y generalización de resultados, emplea instrumentos muy estructurados y estandarizados, como los cuestionarios, escalas, test, etc. otorga una importancia central a los criterios de validez y confiabilidad en relación con los instrumentos empleados, sus diseños de investigación están predefinidos en detalle y son rígidos en su proceso, como los experimentales y *ex post facto y* finalmente por enfatizar la observación de resultados (Sosa, J.R., 2003).

El cuestionario se diseñó acorde a la operacionalización de las variables que definen los objetivos e hipótesis de investigación, el cual contempla 44 reactivos, divididos en 7 secciones:

- Datos generales.
- Información acerca de la gestión de contraseñas de cuentas de usuario.
- Lo referente a descargas.
- Acerca de su información personal.
- Sus hábitos de conexión y actividades en línea.
- Sus esquemas de protección informática.
- Tipo de sistema operativo que utiliza.

Dichos reactivos son del tipo de pregunta cerrada, con escalas Likert, los métodos más conocidos para medir por escalas las variables que constituyen actitudes son: diferencial semántico, escala de Guttman y escalas de Likert (Gómez, M. M., 2006).

Este instrumento *ad hoc* se creó a manera de cuestionario digital a través de Google Forms por las facilidades que otorga para su aplicación y distribución de manera electrónica a los objetos de estudio, así como facilidad de recopilación de datos, para su procesamiento y análisis posterior. Las variables que se consideraron para el instrumento son de tipo categóricas caracterizadas la mayoría en escalas Likert, que se analizarán con estadística cuantitativa no paramétrica con un nivel de significancia del 5% y paramétrica del 1%.

El resultado de la prueba de investigación se aplicó a 39 reactivos, no se consideraron los demográficos o particulares, como se observa en el cuadro, de acuerdo a los autores anteriores, nos muestra una fiabilidad muy aceptable para el instrumento que se aplicó en esta investigación.

Estadísticos de fiabilidad	
Alfa de Cronbach	Número de elementos
.770	39

Fuente: Elaboración propia.

La obtención de la información se realizó con la aplicación de un cuestionario aplicado a los 142 alumnos que conforman el total de las 4 cohortes generacionales de los cuatro semestres de la MTIE del periodo escolar agosto – diciembre 2016, de los cuales solo la contestaron 106 de ellos, lo que constituye nuestro censo. Cabe mencionar que el cuestionario, fue aplicado de manera electrónica en línea a través de Google Forms, la cual es una herramienta que permite recolectar información de usuarios vía un cuestionario personalizado, la información posteriormente a su aplicación puede ser analizada a través de sencillas gráficas y es automáticamente enviada a una hoja de cálculo, con todas las preguntas y sus respuestas correspondientes para ser procesada en otras hojas de cálculo tales como *Calc de LibreOffice*, *Microsoft Excel,* la misma *suite ofimática de Google,* entre otras, o bien, en paquetes de análisis estadístico como *R, SPSS (Statistical Package for the Social Sciences)* o *Statistics*, por mencionar algunos.

Para realizar posteriormente el análisis de la información recabada por el formulario, se recurrió al análisis descriptivo exploratorio univariado y multivariado por medio del Análisis de Componentes Principales (ACP).

Resultados

Al realizar el análisis multivariado de componentes principales, las correlaciones entre las variables representan la confiabilidad de utilizar esta herramienta estadística, es por ello que la prueba de Bartlett nos indican que al aceptar la hipótesis alterna con $p < 0.01$ muestra la significancia de las correlaciones entre las variables, para este caso el valor de Sig. 0.000 (probabilidad de rechazar hipótesis alterna) es menor a 0.01, por lo tanto el instrumento estadístico es adecuado.

Significancia de las correlaciones. KMO y prueba de Bartlett

KMO y prueba de Bartlett		
Medida de adecuación muestral de Kaiser-Meyer-Olkin.		0.581
Prueba de esfericidad de Bartlett	Chi-cuadrado aproximado	1335.818
	gl	703
	Sig.	0.000
Fuente: Elaboración propia		

El cuadro de eigenvalues, muestra los autovalores, los cuales indican la varianza de cada componente, que aparece también expresada en porcentaje de la variabilidad total. La variación explicada de las variables correlacionadas para el primer componente explican el 54.13% de la variabilidad y el segundo el 17.88%. Los dos componentes en conjunto nos explican la variación de las variables correlacionadas en un 72.002%, es decir, podemos explicar el fenómeno con más del 70% de la variación total.

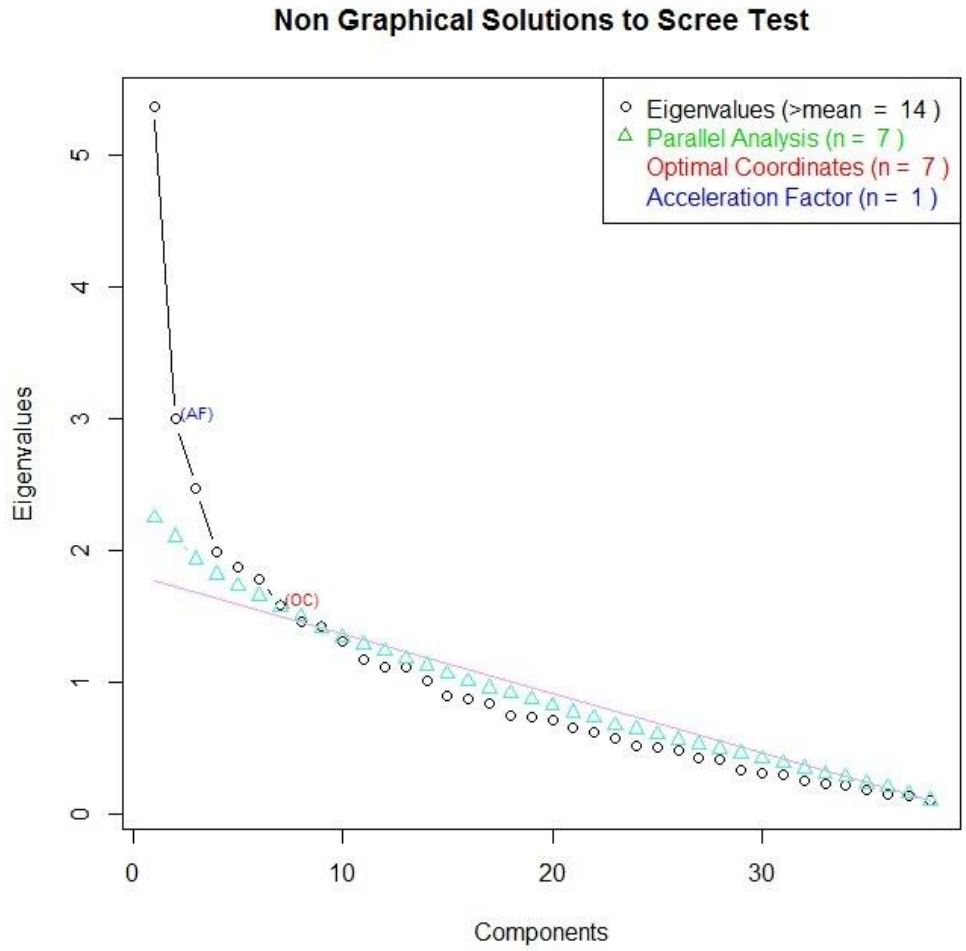
Eigenvalues

	eigenvalue	Porcentaje de varianza	Porcentaje de varianza cumulativa
Comp 1	**5.3673106**	**54.1245017**	**54.1245017**
Comp 2	**2.9936800**	**17.8781053**	**72.0026070**
Comp 3	2.4730397	6.5079993	
Comp 4	1.9888360	5.2337789	
Nota: Se presentan los primeros componentes con significancia.			

Fuente: Elaboración propia.

La gráfica de sedimentación no representa el comportamiento de las variables correlacionadas y la variación explicada que los componentes principales, (en este caso se tomaron 2), lo importante de esta gráfica es observar la pendiente que ésta presenta conforme se aleja del origen, es decir, al principio debe presentar una pendiente pronunciada, y posteriormente ir disminuyendo como se observa en la gráfica 3, lo anterior da certeza de la utilización de este método de análisis estadístico.

Sedimentación



Fuente: Elaboración propia.

El siguiente cuadro muestra el resultado de la matriz de coeficientes o saturaciones de los componentes, que están ordenados por componentes o dimensiones. El primer componente aparece claramente asociado con las variables f5.4, f5.6 y f5.10, las cuales nos representan la primera, la actualización del software antimalware, la segunda, el escaneo de dispositivos (computadoras,

móviles, almacenamiento externo y correos electrónicos) con software antimalware y la tercera, navegar por la Internet utilizando la característica de “navegación privada”. El segundo componente tiene principalmente asociadas a la f2.2, f3.3 y f5.7, las cuales nos indican para el primer caso descargas de archivos de la red de pares P2P, en el segundo caso dar información a desconocidos en las salas de charla y sistemas de mensajería instantánea y por último, utilización de medios de almacenamiento externo propios o de extraños sin cuidado alguno.

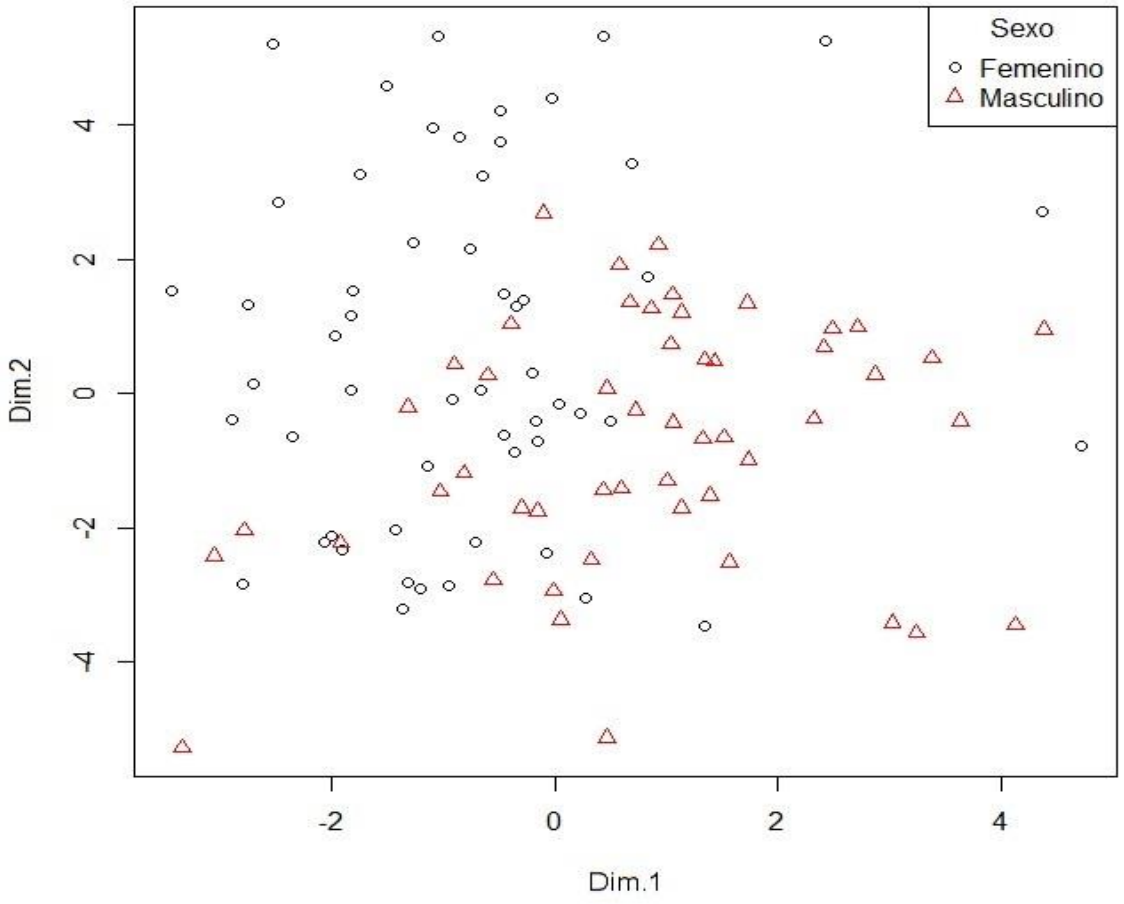
Matriz de componentes

	Dim. 1	Dim.2
f1.7	0.189248719	0.040216682
f2.1	0.188164185	0.363424836
f2.2	-0.089171102	**0.470865078**
f2.3	-0.029687502	0.383434705
f3.2	0.124047294	0.310262211
f3.3	0.027755551	**0.446537909**
f5.3	0.661490513	-0.248637626
f5.4	**0.720270522**	-0.203020126
f5.5	0.542124628	-0.143875231
f5.6	**0.755482128**	-0.164069129
f5.7	0.085852438	**0.494834099**
f5.8	0.454552790	-0.214867959
f5.9	0.628234250	-0.052447042
f5.10	**0.673415653**	0.001834818
f5.14	-0.231228148	0.360696110

Fuente: Elaboración propia.

La gráfica nos muestra la diferenciación por sexo de los alumnos del programa académico, donde podemos observar que los alumnos de sexo masculino tienen mayor incidencia en el componente horizontal y para el componente vertical la mayor incidencia es la del sexo femenino.

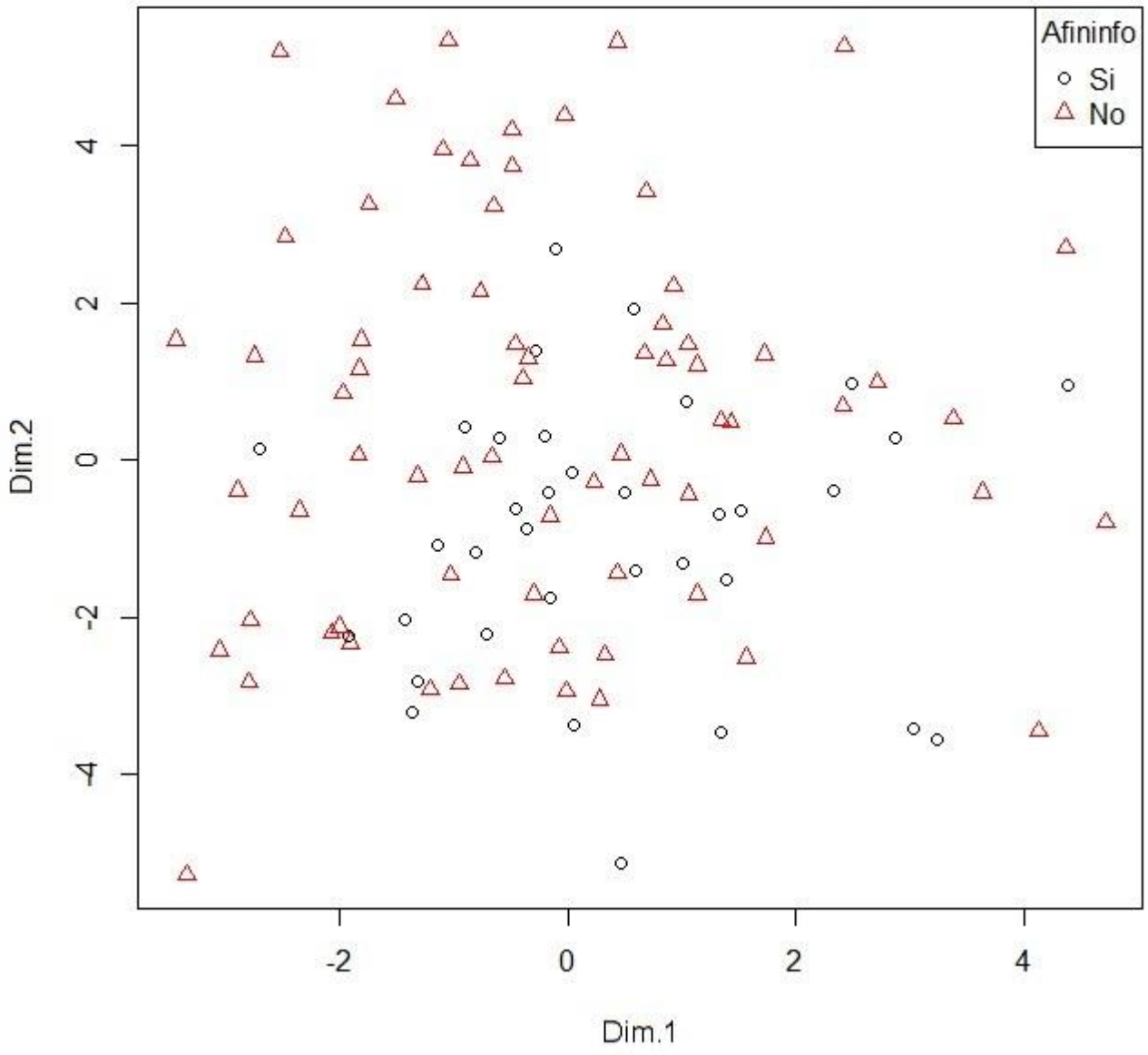
Diagrama de análisis por sexo



Fuente: Elaboración propia

La gráfica siguiente nos muestra la diferenciación de la afinidad a la informática de los alumnos del programa académico, donde podemos observar que los alumnos que tienen licenciatura afín a las áreas de la informática tienen mayor incidencia en el segundo componente, no observando diferenciación para el primer componente.

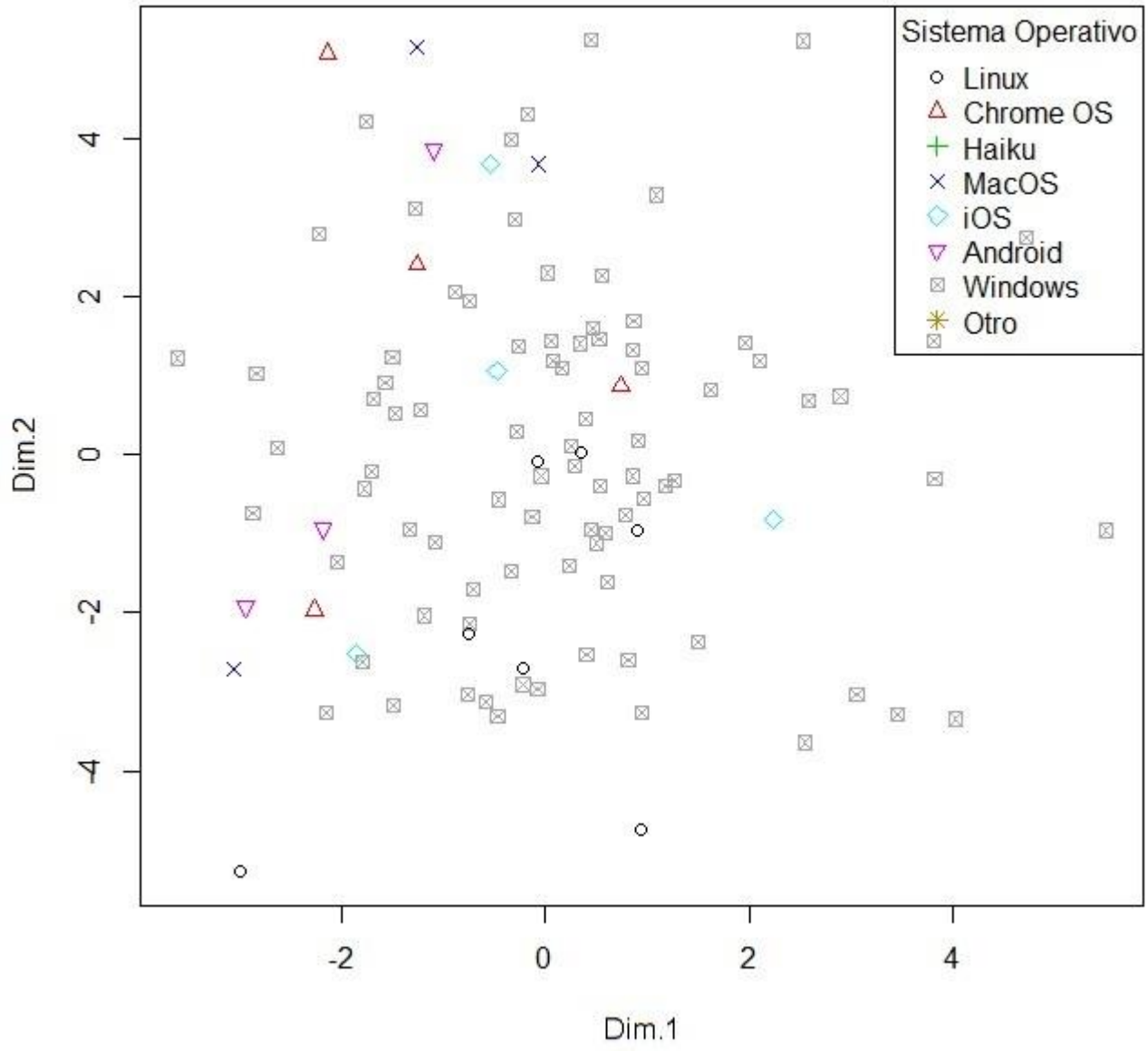
Diagrama de análisis por afinidad a la informática



Fuente: Elaboración propia

Se aprecia en la gráfica la diferenciación por sistema operativo utilizado por los alumnos, donde podemos observar que el S. O. Windows es significativo en ambos componentes.

Diagrama de análisis por sistema operativo



Fuente: Elaboración propia

Conclusiones

La seguridad en todos los aspectos ha sido siempre una prioridad del ser humano desde los inicios de su historia para garantizar su supervivencia y ésta preocupación se ha ido transformando de acuerdo a la evolución de la especie y los avances tecnológicos que la acompañan, en nuestros días, uno de los avances más significativos que ha logrado la humanidad es la Internet que se apoya en las TIC como pilar de su funcionamiento y que se encuentra inmersa en todas las actividades que desarrollan las personas hoy día.

Podemos concluir que de acuerdo a los componentes encontrados en el análisis factorial, los cuales los definimos como; componente 1: estrategias de protección por parte del alumno, las cuales incluyen las variables significativas de actualización de anti-Malware, análisis de dispositivos y navegación de incógnito o privada, y para el componente 2: Métodos de contagio y fuga de información, las variables relevantes son descargas de archivos de servicios de red de pares (P2P), dar información a extraños en salas de chat o SMS y el uso de dispositivos de almacenamiento secundario propios y de terceros sin precaución.

Al comparar estos componentes con las variables principales del estudio y en congruencia con la hipótesis de investigación concluimos lo siguiente: La hipótesis planteada se comprueba en su totalidad, es decir, los alumnos con afinidad a la informática o con antecedentes de informática parecen estar mejor preparados para enfrentar cierto tipo de amenazas, pues muestran una mayor preocupación por tener actualizado su anti-Malware, al respecto del análisis de Malware en sus dispositivos tienen un comportamiento muy similar a los que no son afines a las áreas informáticas, para descargas de redes de pares (P2P) son los de afinidades informáticas quienes lo hacen con mayor frecuencia lo que los hace más vulnerables en este tópico en particular, sin embargo, muestran un mejor nivel de conciencia que los no afines acerca de no facilitar su información personal a extraños por medios digitales de comunicación y al utilizar sus medios de almacenamiento externos con mayor precaución, lo que demuestra que la educación es la mejor estrategia para combatir las cuestiones de seguridad informática, situación que viene a corroborar el estudio de White et al., (2013).

Cabe resaltar que tanto los estudiantes de carreras afines a la informática y los que no lo son, requieren una mejor instrucción o concientización al respecto de la navegación privada, para mejorar sus estrategias de protección, sobre todo por que la mayoría utiliza un sistema operativo que se caracteriza por estar denominado como el más vulnerable, que pertenece a Microsoft, en coincidencia de lo que afirman Clarke et al., (2009) respecto a que el sistema operativo que predomine en determinado momento es aquel que tendrá el mayor número de ataques dirigidos.

Por otra parte, se comprueba que las mujeres tienden a realizar acciones menos cuidadosas de protección, es decir, no emplean estrategias encaminadas a tener mayor seguridad, pues actualizan con menor frecuencia el software anti-malware, analizan con menor frecuencia sus dispositivos de almacenamiento en busca de amenazas de malware y la mayoría de ellas no emplea la navegación anónima/privada.

Por último, podemos agregar que el uso indiscriminado de sistema operativo Windows pone en riesgo a la gran mayoría de los alumnos de la maestría en tecnología informática educativa, ello se demuestra al existir la preocupación de tener siempre actualizado el anti-malware, realizar análisis de sus memorias de almacenamiento externo por la gran mayoría de los estudiantes, por otro lado, el uso sin cuidado de memorias en sus equipos prevalece en este sistema operativo así como la tendencia a no navegar de manera anónima/privada, a pesar de utilizar un sistema operativo de los más vulnerables.

Referencias bibliográficas

Barrón, H. S. (2004). La educación en línea en México. *Revista electrónica de tecnología educativa*, *18*. Recuperado a partir de http://www.quadernsdigitals.net/datos_web/hemeroteca/r_11/nr_180/a_8868/8868.pdf

Clarke, R., Dorwin, D., & Nash, R. (2009). Is open source software more secure? *Homeland Security/Cyber Security*. Recuperado a partir de http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.460.4134&rep=rep1&type=pdf

Davis, M. A., Bodmer, S., & LeMasters, A. (2009). *Hacking Exposed.* New York, USA: McGraw-Hill Professional Publishing. Recuperado a partir de http://public.eblib.com/choice/publicfullrecord.aspx?p=4657740

Espinar Ruiz, E. E. R., & López Fernández, C. L. F. (2009). Jóvenes y adolescentes ante las nuevas tecnologías: percepción de riesgos. *Athenea digital: revista de pensamiento e investigación social*, (16), 001–020.

Gómez, M. M. (2006). *Introducción a la Metodología de la Investigación Científica*. Córdoba, Argentina: Brujas.

Mensch, S., & Wilkie, L. (2011). Information Security Activities of College Students: An Exploratory Study. *Academy of Information & Management Sciences Journal*, *14*(2), 91–116.

Organización de las Naciones Unidas. (2015, marzo). UCentro de noticias de la ONU en español - ONU autoriza relatoría especial sobre el derecho a la privacidad. Recuperado el 7 de abril de 2017, a partir de http://www.un.org/spanish/News/story.asp?NewsID=31995#.WOe_2ke1vdG

Sosa, J.R. (2003). Paradigmas, enfoques y métodos en la investigación educativa. Investigación Educativa, 7(12), 23–40.

Staksrud, E., Livingstone, S., Haddon, L., & Ólafsson, K. (2012). *What do we know about children's use of online t echnologies?: a report on data availability and research gaps in Europe [2nd edition]* (2nd.).

Velasco Melo, A. H. (2008). El Derecho Informático Y La Gestión De La Seguridad De La Información Una Perspectiva Con Base En La Norma Iso 27 001. *Revista de Derecho*, (29), 333–366.

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

Young Susan & Aitel Dave. (2004). *The Hacker's Handbook - The Strategy behind Breaking into and Defending Networks.* Auerbach Publications.