ESTUDIO DESCRIPTIVO DEL *MALWARE* EN UNA DEPENDENCIA ACADÉMICA DE UNA INSTITUCIÓN PÚBLICA DE EDUCACIÓN SUPERIOR

(Descriptive study approach to malware in an academic dependence of a public institution of higher education)

Jesús Ramírez Sánchez*
Teresa García López**
Juan Carlos Bocarando Lara***

Fecha de recepción: 12-04-2016 Fecha de aceptación: 19-08-2016

RESUMEN

En las organizaciones, la información en todas sus formas de presentación, puede considerarse como uno de los recursos fundamentales que permite a los responsables de dirigirlas reducir la incertidumbre al momento de la toma de decisiones en un entorno altamente cambiante, de aquí, la importancia de contar con medidas de seguridad informática para mantenerla con calidad en el momento, lugar y con la exactitud que se requiera. El *Malware*, generalmente denominado *software* malicioso, son programas informáticos sumamente dañinos creados con el interés de dañar a la computadora o a la información contenida en la misma. Tomando en cuenta lo anterior, se consideró pertinente realizar un estudio cuyo objetivo fue identificar los efectos y el impacto que puede ocasionar el *Malware* a los usuarios (directivos, docentes y administrativos) de equipos de cómputo de la Facultad de Contaduría y Administración de la Universidad Veracruzana región de Xalapa, Veracruz con la finalidad de aportar a las autoridades escolares información que sirva de base para tomar medidas al respecto. Entre los hallazgos más relevantes se encontraron algunas limitantes por parte del usuario en los conocimientos con los que cuentan para prevenir los ataques de este tipo de programas, aunado a la costumbre en el uso sin prevención de dispositivos de almacenamiento externo y aplicaciones riesgosas.

Palabras Clave: *Malware*, computadoras personales, usuario.

ABSTRACT

In organizations, information in all forms of presentation can be considered as one of the key resources that allows managers to direct them reduce uncertainty when making decisions in a rapidly changing environment, hence, the importance of have security measures to maintain quality at the time, place and with the accuracy required. Malware, often called malicious software, are extremely harmful computer programs created in the interest of damage to the computer or the information contained therein. Given the above, it was considered appropriate to conduct a study aimed at identifying the effects and impact that can cause the Malware users (principals, teachers and administrators) of computer equipment of the Facultad de Contaduría y Administración de la Universidad Veracruzana región de Xalapa, Veracruz in order to provide information to school authorities as a basis for taking action. Among the most important findings, some limitations by the user on the knowledge at their devices to prevent attacks such programs, coupled with the custom in use without preventing external storage devices and risky applications was found.

Keywords: *Malware, personal computers, user*

*Académico de tiempo completo en la Facultad de Contaduría y Administración, Universidad Veracruzana. jesusramirezsanchez@hotmail.com.
** Investigadora de tiempo completo en Instituto de Investigaciones y Estudios Superiores de las Ciencias Administrativas, Universidad Veracruzana. tgarcia@uv.mx.
*** Alumno de tiempo completo del Doctorado en Planeación Estratégica y Dirección de Tecnología de la UPAEP. larabojcarlos@gmail.com

I. INTRODUCCIÓN

Actualmente, Internet es la red más grande de información con alcance mundial, presente en la mayoría de los hogares, en la vía pública y casi de manera imprescindible en las organizaciones. Con el paso del tiempo los avances tecnológicos han coadyuvado a que se convierta en el medio de acceso a la información y comunicación más explotado pues las ventajas que presenta son diversas, entre ellas, el comercio electrónico, las redes sociales, el correo electrónico, la mensajería instantánea, el acceso a cualquier fuente de información como libros, revistas, noticias, periódicos, documentales, etc., la descarga de archivos multimedia (películas, música, imágenes, etc.), entre los más relevantes.

No obstante, existen desventajas muy serias entre las cuales se pueden mencionar la dependencia de los usuarios para la obtención de información o realización de tareas a través procesos digitalizados y de la energía eléctrica o bien, información recabada de fuentes poco confiables, pero entre la más destacable y motivo de esta investigación, es el *software* malicioso, mejor conocido como *Malware.*

Al respecto, se puede decir que entre los muchos riesgos que se pueden presentar ante esta amenaza, se encuentra la pérdida de información, contratiempos en la ejecución de actividades y de procesos, además de pérdidas monetarias. Así pues las medidas que una organización puede tomar para combatir este tipo de *software* pueden ser inadecuadas o en su defecto estar desactualizadas, por lo que estudiarlas cobra relevancia considerando que puede llegar a afectar a la información.

Ahora bien, el Malware se puede definir como "todo aquel *software* que perjudica a la computadora […]" (Fuentes, 2008), "que no se limita a los virus" […] (Panda Security, 2016) y que puede estar conformado también por "*spyware* y cualquier otro tipo de *software* potencialmente no deseado" (Microsoft, 2016).. Por lo señalado, el estudio tiene como finalidad conocer y describir las medidas que se toman para prever daños ocasionados por éste tipo de *software* y, en aquellos casos en los que se presenta vulnerabilidad de los sistemas informáticos, determinar cuáles son los efectos que origina en la población sujeta a estudio.

II. MALWARE

Se puede decir que es un vocablo que se origina del nexo de dos palabras de procedencia inglesa (*malicious software*). El también llamado "*software* de actividades ilegales es una categoría de código malicioso que incluye virus, gusanos y caballos de Troya" (Symantec Corporation, 2015), además se refiere a todo aquel *software* cuyo objetivo está en corromper la estructura del sistema operativo , así como recolectar información personal de usuarios de manera ilegítima, hasta el empleo de recursos de forma remota (Ramírez Gutiérrez & Reyes Fuentes, 2009, pág. 9).

Es importante precisar que si bien un virus informático es un *software* malintencionado que se asocia a otros programas computacionales o archivos informáticos para poder ejecutarse, por lo general sin el conocimiento o permiso del usuario (Laudon & Laudon, 2012, pág. 296), cuando nos referimos al *software* malicioso, aludimos a un cúmulo de amenazas que afectan a los sistemas de cómputo, es decir, puede tratarse de un virus, un caballo de Troya, una puerta trasera (*backdoor*), un programa espía (*spyware*), hasta un devastador gusano que puede echar abajo toda una infraestructura de red (Fuentes, 2008, pág. 4).

Como un breve antecedente de este concepto, se puede mencionar (PandaLabs, 2015):

> En 1972 el científico informático Robert Thomas Morris creo el primer virus informático al cual llamó *Creeper* (enredadera), diseñado para atacar los computadores IBM 360, este *Malware* emitía en intervalos de tiempo el mensaje "Soy una enredadera… ¡atrápame si puedes!", entonces para poder suprimir al *Creeper* se programó lo que sería el primer antivirus al cual se le llamó *Reaper* (segadora).

Poco a poco el *Malware* fue evolucionando hasta ser uno de los agresores más temidos por los usuarios de las Tecnologías de la Información y la Comunicación (TIC) es decir, "recursos, herramientas y programas que se utilizan para procesar, administrar y compartir la información mediante diversos soportes tecnológicos" (Universidad Nacional Autónoma de México, 2013), considerando que son programas para impactar en forma negativa desde las más imponentes organizaciones hasta al usuario promedio que necesita utilizar las computadoras para realizar sus actividades cotidianas y alcanzar sus metas personales y laborales.

El uso creciente de los sistemas informáticos ha causado que los *hackers* se sientan más atraídos a atacar las vulneraciones de las TIC mediante malas prácticas que afectan tanto a individuos como a empresas, ya sea para obtener un beneficio o sólo por el puro goce de perjudicar lo ajeno. Sin embargo, el problema no radica únicamente en esta situación, sino también en el hecho de lo que no se está haciendo para evitar que las intrusiones no deseadas sean nulas o cuando menos impedir que éstas no puedan

obtener ningún tipo de información que cause perjuicios.

Mientras tanto, el Presidente de *Unisys* en Latinoamérica, Helcio Beninatto comentó que en México, el sector financiero es de los más afectados en lo que a delitos cibernéticos se refiere:

> La encuesta *Unisys Security Index* 2014 en México reveló que tres cuartas partes de los mexicanos (75%) están seriamente preocupados por la posibilidad de que algún delincuente use la información personal de sus tarjetas de crédito y/o débito, y el 86% están principalmente preocupados por el robo de identidad (Beninatto, 2014).

Está claro que los avances constantes en las TIC no sólo se exhiben de manera positiva sino que también tiene su contraparte, en este caso el *software* malicioso, el cual también sufre innovaciones, está en constante desarrollo, afecta y se manifiesta en todo el mundo.

Un estudio realizado por Bugarini (2007, pág. 83), sobre una propuesta de seguridad en la información, demostró que los usuarios de dicha organización no contaban con los elementos ni la cultura informática necesaria para salvaguardar la información que manejan. Se destaca también, que se carecen de medidas adecuadas y que falta conciencia del tema de la seguridad informática y protección de información a nivel organizacional.

Mientras tanto Domínguez (2009), realizó una investigación acerca del *Malware* y sus efectos en las organizaciones de la región de Xalapa, encontrando que en aquellas organizaciones (privadas o públicas) que tuvieron estragos a causa de este tipo de *software* las consecuencias más importantes fueron la pérdida de tiempo, así como las pérdidas monetarias y las afectaciones a los clientes.

Por lo que se refiere a la presente investigación, se pretende describir los efectos y el impacto que ocasiona el *Malware* a los usuarios de computadoras personales de la Facultad de Contaduría y Administración de la región de Xalapa, Veracruz de una institución pública de educación superior por lo que en el siguiente apartado se narra brevemente la metodología usada para el desarrollo del estudio y posteriormente, se presentan algunos de los resultados obtenidos.

III. METODOLOGÍA

Los elementos metodológicos de mayor relevancia tienen su origen en la pregunta de investigación planteada: ¿cuáles son los efectos e impacto del *Malware* en los usuarios de computadoras personales de la Facultad de Contaduría y Administración de la Universidad Veracruzana región de Xalapa?

En concordancia con la pregunta de investigación, se estableció como objetivo: identificar los efectos y el impacto que puede ocasionar el *Malware* a los usuarios de equipos de cómputo de la Facultad de Contaduría y Administración de la región de Xalapa, Veracruz.

La atención inicial se orientó a considerar como unidad en estudio, a los usuarios de computadoras personales con puestos administrativos, directivos y docentes de la Facultad referida , que son quienes utilizan los equipos de cómputo propiedad de la institución. La información proporcionada por el administrador de la dependencia académica durante el período de estudio (enero – julio de 2015) acerca del capital humano señalado permitió determinar que “son 32 personas las que integraron el sector de directivos y administrativos, mientras que 129 personas el sector de docentes” (Rodríguez García, 2015).

Es importante señalar que las computadoras personales que se tenían registradas en uso los docentes, eran únicamente 90 equipos por lo que éstos últimos fueron los que cumplieron con los requisitos de selección y por lo tanto la población a estudiar quedó conformada por 122 personas (90 docentes así como 32 directivos y administrativos), lo que llevó a la decisión de realizar un censo.

Con base en la pregunta y los objetivos de investigación, se definieron las variables a estudiar, mismas que se detallan a continuación:

1. *Datos generales*: edad, género y sector (directivos, docentes o administrativos).
2. *Uso de antivirus* así como la actualización y mantenimiento de los mismos.
3. *Conocimientos para la prevención del Malware:* comprensión por parte del usuario acerca de las implicaciones del software malicioso.
4. *Uso de dispositivos y aplicaciones riesgosas*: acciones que lleva a cabo el usuario para la protección de dispositivos y aplicaciones que pueden ser afectadas por el *Malware*.
5. *Percepción de mal funcionamiento de software y hardware*: apreciación del usuario acerca de las afectaciones que tiene el *Malware* en su equipo de cómputo y en las aplicaciones instaladas.
6. *Efectos en el desempeño laboral:* percepción del usuario de las consecuencias positivas o negativas en

las actividades laborales por posible software malicioso en las PC.

Con las variables identificadas, se diseñó un instrumentó tipo cuestionario y se determinó que lo más adecuado en el trabajo de campo sería la técnica de la encuesta. Para efectos de evaluar la validez y la confiabilidad del documento referido, se solicitó la opinión de expertos quienes realizaron aportaciones para su mejora, mismas que fueron desde correcciones gramaticales hasta ajustes en la clasificación y adhesión de ítems. La versión final del instrumento se integró de 46 preguntas, de las cuales cuatro fueron abiertas, veinte dicotómicas, seis de opción múltiple y dieciséis de opciones con escala tipo *Likert*.

En tanto la prueba de confiabilidad se llevó a cabo empleando los datos de 30 cuestionarios a través de la versión 22.0 del *software* estadístico de *IBM Statistical Package for the Social Sciences* (SPSS). El Alfa de *Cronbach* obtenido fue de 0.744 lo que refleja un grado excelente de confiabilidad como se puede observar en el cuadro 1.

Cuadro 1.

Niveles de confiablidad con base en Alfa de Cronbach

Parámetros	Grado de confiabilidad
0.53 a menos	Confiabilidad nula
0.54 a 0.59	Confiabilidad baja
0.60 a 0.65	Confiable
0.66 a 0.71	Muy confiable
0.72 a 0.99	Excelente confiabilidad
1.0	Confiabilidad perfecta

Fuente. Herrera, 1998 citado por Ramírez Sánchez, (2014).

Posteriormente, se realizaron las encuestas correspondientes mediante visitas personales a los integrantes de la población a estudiar. Si bien durante las visitas se les explicaba el motivo y el objetivo de la investigación solicitándoles su apoyo y colaboración, numerosos usuarios se mostraron poco dispuestos a responder excusando falta de tiempo o nula autorización para contribuir con actividades de esta índole. A pesar los esfuerzos realizados se lograron obtener únicamente 54 encuestas, lo cual representa aproximadamente el 44 por ciento de la población sujeta a estudio.

A continuación, se enlistan algunas de las respuestas obtenidas durante el trabajo de campo y por las cuales no se obtuvo la información solicitada:

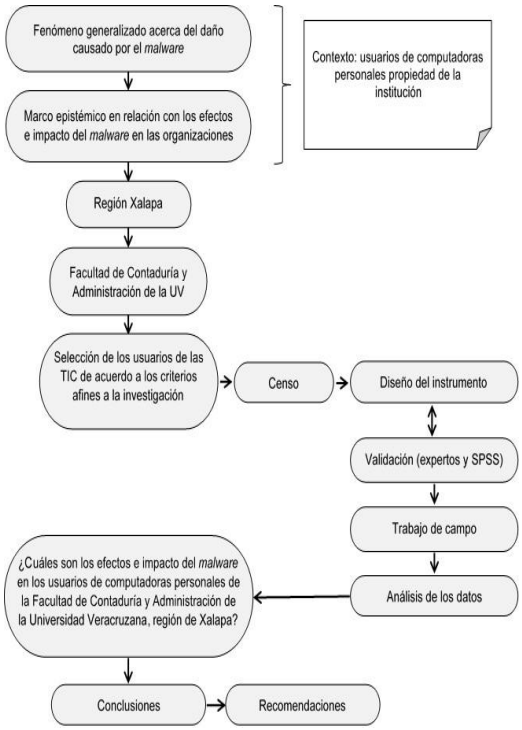
> «No cuento con el tiempo disponible para hacerlo».
> «Déjame la encuesta, pero, no te aseguro poder contestarla».
> «Mi sindicato me prohíbe participar en cualquier actividad externa a mi trabajo, por lo tanto no puedo contestar tu encuesta».
> «Voy de salida, ven después».
> «Ya escuche de qué se trata y la verdad tengo cosas más importantes, disculpa».

A pesar de las limitaciones señaladas, principalmente la falta de disposición por parte de los integrantes de la población sujeta a estudio para responder, se decidió complementarlo con los datos recabados mismos que se analizaron por medio de gráficos y tablas. Posteriormente se realizó la interpretación mediante texto narrativo.

En la figura 1, se muestran las fases de la metodología que se siguió para el desarrollo de la investigación, iniciando con la determinación del fenómeno generalizado y en la definición del contexto (Facultad de Contaduría y Administración de la Universidad Veracruzana región Xalapa) permitiendo identificar las características de la población a estudiar, para decidir llevar a cabo un censo de la misma. Posteriormente al diseño del instrumento de recopilación de información, éste fue validado por expertos en el tema, ajustado de acuerdo con sus sugerencias y determinada su confiabilidad. Por último, se llevó a cabo el análisis de los datos recabados cuya interpretación llevó a responder la pregunta de investigación planteada y posteriormente a proponer algunas conclusiones y recomendaciones.

Figura 1.

Fases de la metodología usada para el desarrollo del estudio



Fuente. Elaboración propia.

IV. RESULTADOS

El análisis de la información que se presenta a continuación está basada en la opinión obtenida de los 54 usuarios que contribuyeron con la investigación, ya que el resto, por distintos motivos se negó a contestar el instrumento. Por tanto, los resultados son tratados como una muestra y en cada apartado se describe a las variables estudiadas.

Datos generales

La edad promedio de los encuestados fue de 41 años con una desviación estándar de 14 años, una mínima de 21 y una máxima de 70 años de edad. El menor promedio de edad corresponde al sector administrativo (35 años), seguido de los directivos (41 años) y por último los docentes con 45 años de edad en promedio.

El 57% de la población en estudio pertenece al género femenino; en la Tabla 1, se presenta la distribución porcentual de acuerdo con el género y el sector al que pertenecen.

Tabla 1.
Distribución por género y sector de los integrantes de la muestra

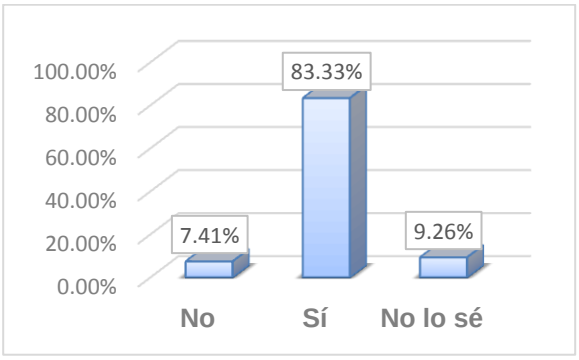
Sector	Femenino		Masculino		Total	
	No.	%	No.	%	No.	%
Administrativo	14	45%	5	22 %	19	35%
Directivo	3	10%	1	4%	4	7%
Docente	14	45%	17	74 %	31	58%
Total general	**31**	**100 %**	**23**	**10 0%**	**54**	**100%**

Fuente. Elaboración propia con datos de la encuesta.

Uso de antivirus

Con relación a los conocimientos del usuario acerca de los programas diseñados para contrarrestar el *Malware* así como la actualización y el mantenimiento de los mismos, se encontró que el 83.3% de los encuestados afirmó que la computadora está protegida con un antivirus y solamente un 7.4% y 9.3% dijeron que no está protegida o que no lo saben, respectivamente (Ver Gráfica 1).

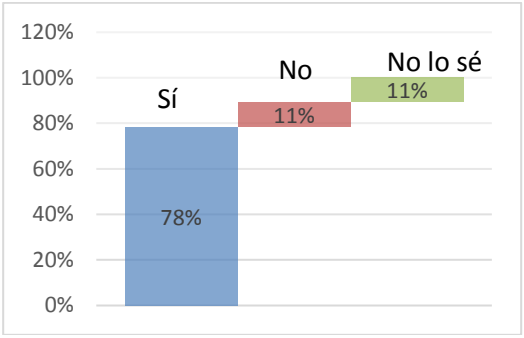
Gráfica 1.
Encuestados que dijeron contar con protección antivirus



Fuente. Elaboración propia con datos de la encuesta.

El 78% de los encuestados mencionaron que el antivirus instalado en su computadora, recibe mantenimiento permanente, pero un 22% afirmó que no o que no sabe si lo tiene. Día con día aparecen nuevos virus informáticos y si las herramientas que los combaten no están actualizadas, entonces podría decirse que se trata de un equipo vulnerable (Ver Gráfica 2).

Gráfica 2.
Mantenimiento del antivirus instalado



Fuente. elaboración propia.

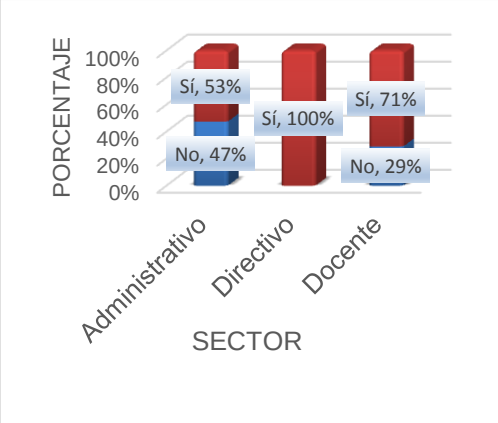
A pesar de lo mencionado, únicamente el 65% del total de los encuestados dijo conocer las causas por las que se propaga el software malicioso y el 52% tener conocimientos acerca de aplicar técnicas que prevengan el contagio.

Conocimientos para la prevención del Malware

Inicialmente se les consultó a los encuestados acerca de su conocimiento sobre el *Malware* y se encontró que todos los directivos manifestaron conocer el concepto. Asimismo, un mayor porcentaje de administrativos (47%) que de docentes (29%), señalaron no conocer lo que es el *Malware* (Ver Gráfica 3).

Sin embargo es importante mencionar que el 33.33% del total, declaró no conocer el significado de Malware.

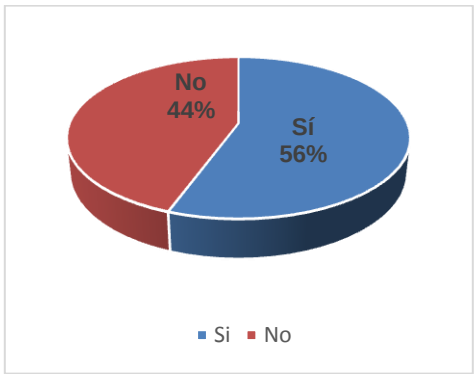
Gráfica 3.
Distribución porcentual acerca del conocimiento que tienen los encuestados sobre el Malware



Fuente. Elaboración propia con datos de la encuesta.

Un 44% de los trabajadores afirmó no haber recibido información sobre los riesgos del software malicioso (Ver Gráfica 4). De acuerdo con estos datos, se podría inferir que no existe un programa de capacitación formalmente establecido para preparar al capital humano acerca de este tipo de riesgos, y los que conocen posiblemente es por aprendizaje propio.

Gráfica 4.
Información recibida acerca del Malware



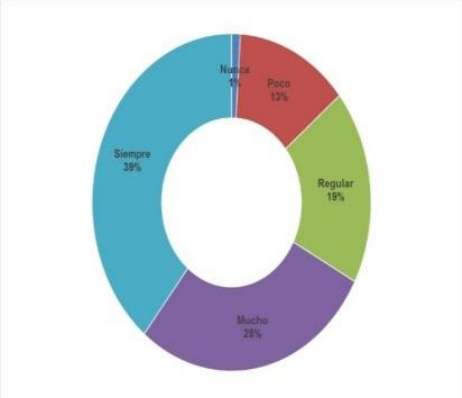
Fuente. Elaboración propia con datos de la encuesta.

Uso de dispositivos y aplicaciones riesgosas.

Los dispositivos de almacenamiento externo pueden ser una fuente de contaminación por malware, puesto que tienen la característica de poder ser conectados en diversos equipos cuantas veces sea necesario, por lo que se vuelven vulnerables ante computadoras afectadas.

Con relación a las aplicaciones o *software* que puede ser afectado por el *Malware*, se consultó a los encuestados si acostumbran bajar a sus computadoras los archivos digitales que acompañan al correo electrónico. Solamente el 14% de los trabajadores dijeron no bajar archivos que acompañan al correo electrónico, con lo que la mayoría (86%), se encuentra ante el riesgo de software malicioso que pueda venir oculto en los mencionados archivos digitales (Ver Gráfica 5).

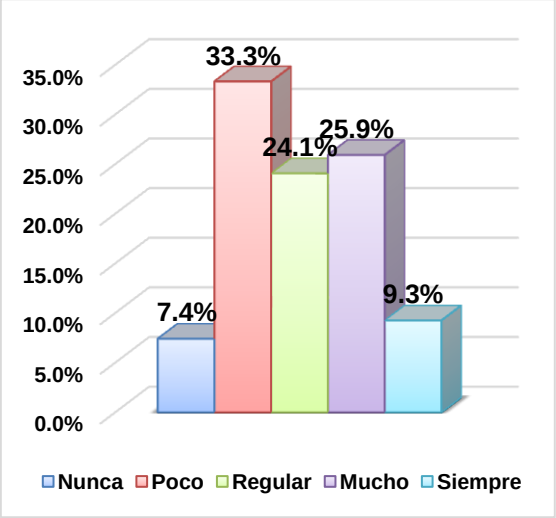
Gráfica 5.
Distribución porcentual de los encuestados que acostumbran bajar a su computadora archivos que acompañan al correo electrónico



Fuente. Elaboración propia con datos de la encuesta.

En la Gráfica 6, se muestra que únicamente el 7.4% de los encuestados dijeron nunca recibir información sospechosa por medio del correo electrónico y un 33.3% dijo que pocas veces; sin embargo, el 24.1% dijo que la recibe de manera regular, el 25.9% bastante y un 9.3% que siempre la recibe. Los archivos adjuntos al correo electrónico con características sospechosas, pueden ser ejecutables de *Malware* y deben manejarse con precaución por parte del usuario.

Gráfica 6.
Recepción de documentos sospechosos por medio del correo electrónico

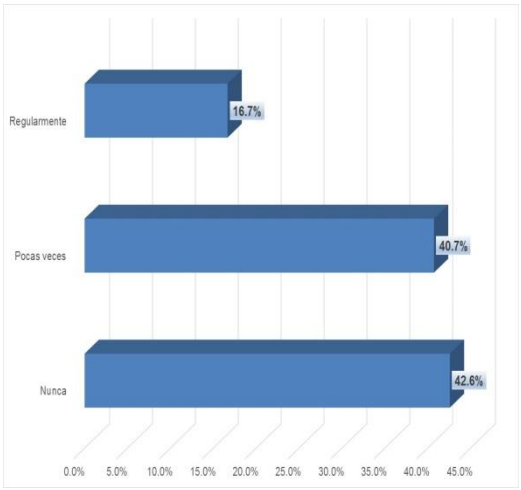


Fuente. Elaboración propia con datos de la encuesta.

Percepción del impacto del Malware en el software y hardware

Con relación a la apreciación del usuario acerca de las afectaciones que tiene el *Malware* en su equipo de cómputo y aplicaciones instaladas, se preguntó a los encuestados la frecuencia con la que han sido víctimas de ataques de software malicioso, las respuestas se muestran en la Gráfica 7, en la que el 42.6% de los encuestados dijeron que nunca han sido atacados por este tipo de programas. En contraposición, el resto de ellos dijeron que pocas veces o que de manera regular le suceden dichos problemas.

Gráfica 7.
Frecuencia de ataques por malware



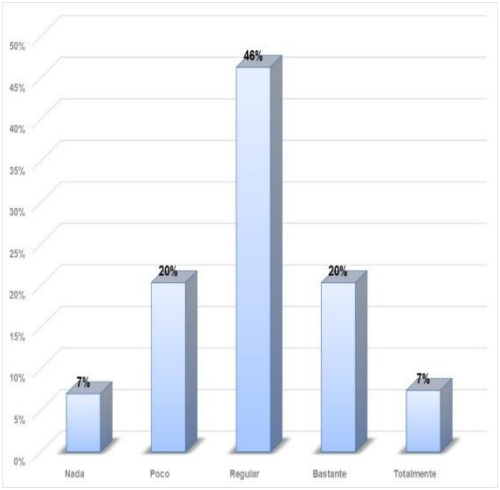
Fuente: elaboración propia con datos de la encuesta.

Sin embargo al consultarles si han escuchado acerca de ataques informáticos recibidos por alguno de los equipos de cómputo de la dependencia, el 57% mencionó haberse enterado de la existencia de éstos.

IV.1 Efectos en el desempeño laboral

La seguridad informática es un tema muy importante dentro de una organización puesto que la información que contienen los equipos de cómputo, es sumamente importante tanto para el usuario como para la misma organización. En este estudio, el 7.4% considera que su información digital se encuentra totalmente segura, el 20.4% bastante segura y el 46.3% afirmó que la seguridad es regular. Únicamente el 20.4% y el 5.6% aseveraron que su información esta poco o nada segura en su computadora (Ver Gráfica 7).

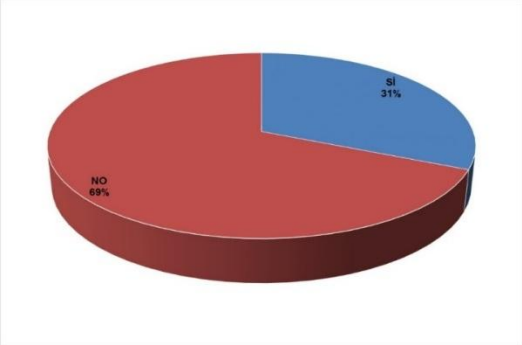
Gráfica 8.
Percepción acerca de la seguridad de la información en la computadora



Fuente: elaboración propia con datos de la encuesta.

Cuando se les consultó acerca de la necesidad de recuperar o rehacer información digital importante relacionada con sus funciones laborales, debido a que ha desaparecido de la computadora sin explicación o de forma repentina, extraña e injustificable, el 31% dijo haberse enfrentado a este tipo de complicaciones ocasionadas por posible s virus en los equipos (Ver Gráfica 9).

Gráfica 9.
¿Ha requerido recuperar o rehacer información laboral importante?



Fuente: elaboración propia con datos de la encuesta.

V. CONCLUSIONES

La información digital puede ser considerada como uno de los activos principales para las organizaciones ya sean públicas o privadas, por lo que la seguridad informática es un tema que debe ser tratado con relevancia considerando la constante evolución de los avances tecnológicos que no sólo generan cambios positivos sino también negativos como el *Malware*.

Considerando la pregunta de investigación acerca de, ¿cuáles son los efectos e impacto del *Malware* en los usuarios de computadoras personales de la Facultad de Contaduría y Administración de la Universidad Veracruzana región de Xalapa?, se puede concluir lo que a continuación se describe.

Las características que identificaron a la población en estudio fueron en su mayoría mujeres del sector docente y con edad promedio de 41 años.

Aunque el 83% de los encuestados dijeron contar con antivirus en su computadora, y el 78% tener mantenimiento de dicho antivirus, es importante considerar que el 35% dijo no conocer las causas por las que se propaga el software malicioso y el 48% no contar con conocimientos para aplicar técnicas que prevengan el contagio.

El 44% de los encuestados manifestó no haber recibido ningún tipo de capacitación o asesoramiento acerca de cómo defender y salvaguardar su información digital, por otro lado, la tercera parte de los encuestados desconocieron el concepto de *Malware*.

A pesar de que casi el 60% de los trabajadores señalaron recibir a través del correo electrónico información sospechosa, el 86% tiene la costumbre de bajar a su computadora la información que acompaña a sus correos.

El 31% de los trabajadores, dijo haberse enfrentado a la necesidad de recuperar o rehacer información digital importante relacionada con sus funciones laborales, debido a que ha desaparecido de la computadora sin explicación o de forma repentina, extraña e injustificable. También es importante concluir que el 72% consideró la seguridad de su información regular o mala.

Finalmente, con base en lo anterior se puede decir que la dependencia académica requiere un esquema de seguridad informática con mayores medidas de prevención y salvaguarda de la información que evite posibles daños a la misma por *software* malintencionado. Aunque en la dependencia estudiada el impacto y los efectos del *Malware* parecen no ser de índole totalmente negativa es conveniente mencionar que los resultados indican la importancia de capacitar e informar a los usuarios para que puedan afrontar los posibles efectos negativos de este tipo de programas.

VI. REFERENCIAS

Beninatto, H. (20 de Octubre de 2014). *FORBES*. Obtenido de http://www.forbes.com.mx/seguridad-financiera-y-fraude-debes-preocuparte/

Bugarini Hernández, F. (31 de Octubre de 2007). *Una propuesta de seguridad en la información: caso Systematics de México S.A.* (I. P. Nacional, Ed.) Recuperado el 18 de Febrero de 2015, de Repositorio electrónico del Instituto Politécnico Nacional. Tesis nivel posgrado: http://tesis.ipn.mx/dspace/bitstream/123456789/498/1/TESIS%20PROPUESTA%20SEGURIDAD.pdf

Domínguez Frausto, J. E. (Julio de 2009). *El malware y sus efectos en las organizaciones de la región de Xalapa.* Recuperado el Noviembre de 2015, de Universidad Veracruzana: http://cdigital.uv.mx/bitstream/123456789/28497/1/Dominguez%20Frausto.pdf

ESET Research. (18 de Diciembre de 2014). Obtenido de We Live Security: http://www.welivesecurity.com/la-es/2014/12/18/tendencias-cibercrimen-predicciones-2015/

Fuentes, L. F. (10 de abril de 2008). Malware, una amenaza de Internet. *Revista Digital Universitaria, 9*(4), 1-9.

KasperskyLab. (9 de Diciembre de 2015). *Kaspersky Lab: registro de nuevos programas maliciosos bajó a 310.000 por día en 2015 a la par que cibercriminales buscan ahorrar dinero.* Recuperado el Enero de 2016, de Comunicados de Prensa: http://latam.kaspersky.com/sobre-kaspersky/centro-de-prensa/comunicados-de-prensa/2015/registro-de-nuevos-programas-maliciosos-bajo-a-310000-por-dia-en-2015

Laudon, K., & Laudon, J. P. (2012). *Sistemas de Información Gerencial* (Doceava edición ed.). México: Pearson Educación.

Microsoft. (2016). *Proveedores de software de seguridad para particulares*. Recuperado el 27 de Febrero de 2014, de Windows: http://windows.microsoft.com/es-es/windows/antivirus-partners#AVtabs=win7

Orenday, R. (11 de Noviembre de 2014). *Forbes*. Recuperado el 1 de Marzo de 2015, de http://www.forbes.com.mx/proteccion-de-datos-personales-como-un-activo-en-tu-negocio/

Oviedo, H. C., & Campo-Arias, A. (2005). Metodología de investigación y lectura crítica de estudios. Aproximación al uso del coeficiente Alfa de Cronbach. *Revista Colombiana de Psiquiatría, XXXIV*(4), 572-580 . Obtenido de http://www.redalyc.org/pdf/806/80634409.pdf

Panda Security. (2016). *Antimalware: La solución perimetral en tiempo real contra los códigos maliciosos*. Recuperado el Julio de 2015, de Panda Soluciones de seguridad: http://www.pandasecurity.com/mexico/enterprise/solutions/security-appliances/anti-malware.htm

PandaLabs. (2015). *Classic Malware: su historia, su evolución*. Recuperado el 10 de marzo de 2015, de Panda security: http://www.pandasecurity.com/spain/homeusers/security-info/classic-MALWARE/

Ramírez Gutiérrez, R. O., & Reyes Fuentes, O. A. (2009). *Implementación de un laboratorio de análisis de Malware.* México D.F.: UNAM.

Ramírez Sánchez, J. (2014). *La calidad de vida en relación con el uso de las redes sociales electrónicas: un estudio de percepción de los estudiantes de bachillerato en la ciudad de Xalapa, Veracruz. Tesis de Doctorado.* Puebla: Universidad Autónoma del Estado de Puebla.

Rodríguez García, V. M. (2015). Personal de la población sujeta a estudio. (F. García Montero, Entrevistador)

Symantec Corporation. (2015). *Cómo atacan: malware*. Recuperado el 10 de junio de 2015, de Norton: http://mx.norton.com/security_response/malware.jsp

Universidad Nacional Autónoma de México. (2013). *¿Qué son las TIC?* Recuperado el 15 de Julio de 2015, de Colegio de Ciencias y Humanidades: http://tutorial.cch.unam.mx/bloque4/lasTIC