Factores que influyen en la implementación del Hacking ético en una organización

M.A.E. Torres-Mansur, Sandra Maribel[1]; M.I.A. Placeres-Salinas, Sandra Imelda [2]; M.A.E. Barrera Espinosa, Azalea[3]

[1] Universidad Autónoma de Nuevo León, Facultad de Contaduría Pública y Administración (México), sandra.torresmn@uanl.edu.mx, Av. Universidad S/N, Ciudad Universitaria, San Nicolás de los Garza, Nuevo León, México, +52 1 81 1610 0946
[2] Universidad Autónoma de Nuevo León, Facultad de Contaduría Pública y Administración (México), sandra.placeressl@uanl.edu.mx, Av. Universidad S/N, Ciudad Universitaria, San Nicolás de los Garza, Nuevo León, México, +52 1 81 8309 1160
[3]Universidad Autónoma de Nuevo León, Facultad de Contaduría Pública y Administración (México), azalea.barreraes@uanl.edu.mx, Av. Universidad S/N, Ciudad Universitaria, San Nicolás de los Garza, Nuevo León, México, +52 1 81 1965 7492

Información del artículo arbitrado e indexado en Latindex:
Revisión por pares
Fecha de publicación: Julio 2019

Resumen

En las organizaciones cada vez son más utilizadas las Tecnologías de Información y Comunicación las cuales aportan muchos beneficios, pero a la vez traen consigo riesgos inminentes que el administrador de una organización debe contemplar para asegurar la protección de la información de esta. El propósito de la presente es conocer las variables que debe considerar el administrador de una organización para la implementación exitosa del hacking ético, para crear un instrumento partiendo de la opinión de los expertos en tecnologías de información utilizando el Método Delphi. Se propone un modelo que contempla el conocimiento y experiencia, los recursos e infraestructura, la ética del Hacker y el compromiso de la administración; además se realizó un muestreo no probabilístico donde se confirmó que dicho instrumento es pertinente para el objeto de estudio.

Palabras clave: Hacking ético / organización / implementación

Abstract

En las organizaciones cada vez son más utilizadas las Tecnologías de Información y Comunicación las cuales aportan muchos beneficios, pero a la vez traen consigo riesgos inminentes que el administrador de una organización debe contemplar para asegurar la protección de la información de esta. El propósito de la presente es conocer las variables que debe considerar el administrador de una organización para la implementación exitosa del hacking ético, para crear un instrumento partiendo de la opinión de los expertos en tecnologías de información utilizando el Método Delphi. Se propone un modelo que contempla el conocimiento y experiencia, los recursos e infraestructura, la ética del Hacker y el compromiso de la administración; además se realizó un muestreo no probabilístico donde se confirmó que dicho instrumento es pertinente para el objeto de estudio.

Palabras clave: Hacking ético / organización / implementación

1. INTRODUCCIÓN

Las tecnologías de información han tomado un papel cada vez más importante en los procesos de negocios, creando así nuevas necesidades, impulsando el desarrollo de nuevos productos y servicios e instituyendo nuevos procedimientos (Stephen, 2000).

Así mismo, para la Gerente de Security Solutions & Education (SSE), representantes para Colombia en el Consejo Internacional de Comercio Electrónico, comenta que "es necesario comprometerse con la protección de la información a nivel empresarial tanto organizaciones pequeñas, medianas y grandes que manejan su sistema de información por medio de internet y de dispositivos electrónicos deben de hacer un análisis de vulnerabilidades al menos una vez al año" (Enter.co, 2014).

Debido a lo anterior uno de los servicios que ha cobrado mayor relevancia es la aplicación del Hacking ético en las organizaciones, el cual consiste en contratar expertos para implementar técnicas de intrusión bajo un ambiente controlado con el fin de conocer cómo se puede infiltrar en la red un atacante real, esta simulación permite encontrar brechas y riesgos en la seguridad, las cuales pueden ser usadas para manipular información o suplantar identidades. Como resultado de estas pruebas, los administradores o gerentes podrán tomar decisiones para realizar mejoras en las configuraciones y accesos a la información (Hurtado, y Mendaño, 2016).

Sin embargo, en la mayoría de los casos el hacking ético se aplica de manera reactiva y no preventiva, como debería de ser (Rodríguez, 2016). Según un estudio hecho por KPMG en el año 2006 y 2010 relacionado al fraude en México, menciona que 8 de cada 10 empresas han sido afectadas y las organizaciones no están tomando las medidas de seguridad necesarias para poder enfrentar los riesgos que se presentan (Guevara, 2012).

Por otra parte según la Comisión Nacional para la protección y Defensa de los Usuarios de los Servicios Financieros (CONDUSEF), los ciberdelitos han superado por mucho al robo de identidad y la clonación de tarjetas. El porcentaje de quejas por fraudes cibernéticos en el periodo de enero-junio del 2018 creció un 25% más con respecto al 2017 en el mismo periodo (Pixel, 2018).

En México existe un bajo índice de inversión por parte de las organizaciones en auditorías de seguridad, ya que según la revista de seguridad en el artículo "Hacking ético y la seguridad de la información de empresas en México" dice que: "No se les presta la debida importancia y se prefiere invertir en otras áreas que puedan redituar a corto plazo". Podemos afirmar que las organizaciones desconocen el impacto que puede generar el que sus sistemas sean violentados (Guevara, 2012).

La aplicación del Hacking ético hoy en día no se ha incrementado en la misma proporción que los ciberdelitos, debido a que las organizaciones tienen cierto temor o incertidumbre de contratar estos servicios (Johansen, 2017); ya que el Hacker ético debe tener acceso abierto a todas las computadoras. Además toda la información, especialmente la técnica y datos deberán estar en el dominio público (Bissett, 2003).Debido a lo anterior es importante que el administrador de una organización tenga conocimiento de los factores que debe considerar a la hora de contratar los servicios de hacking ético, ya que la protección de la información debe ser parte de su rol. Por lo que el objetivo de esta investigación es conocer las variables que influyen en la implementación exitosa del hacking ético en una organización desde el punto de vista de los especialistas en tecnologías de información, para que los administradores de las organizaciones tengan conocimiento de dichas variables y sepan que esperar a la hora de buscar la contratación del Hacking ético, ya que se prevé que esto siga en franco crecimiento en el corto plazo. La finalidad del presente es validar el instrumento con las variables propuestas, en un muestreo no probabilístico, para posteriormente aplicarlas a una muestra representativa en el área metropolitana de Monterrey.

2. MARCO TEÓRICO

2.1. Hacking ético

Para Saavedra y Tapia (2013), hoy en día es difícil visualizar una empresa exitosa sin el apoyo de las Tecnologías de información y comunicación (TIC). Son muchos los beneficios que las TIC aportan a las organizaciones, pero también trae consigo riesgos que pudieran impactar gravemente en la continuidad de las operaciones de la organización. Por lo que, es importante prevenir dichos riesgos y tener una seguridad informática adecuada (Gil V. & Gil V., 2017).

Uno de los riesgos es el ataque informático; existen diferentes tipos de ataques: ataques activos y pasivos; en el primer tipo se producen cambios en la información y en los

recursos de los sistemas, en el segundo registran el uso de los recursos, también pueden acceder a la información guardada o la que es transmitida a los sistemas; otro riesgo es el robo de información, donde esta es interceptada cuando es enviada entre las diferentes computadoras o dispositivos de la red de comunicaciones del negocio (Gómez, 2014).

"El Hacking ético es una actividad que incluye diversos ataques a redes de computadores en ambientes controlados, donde los responsables de los sistemas a atacar han sido previamente informados y han autorizado los mismos con el fin de establecer el estado de inseguridad de su sistema y conocer detalladamente sus vulnerabilidades, los cuales son practicados por profesionales en Seguridad Informática", denominados Hackers éticos (Gacharná, 2009).

Según Gacharná (2009), las organizaciones más afectadas son las que pertenecen al giro bancario o aseguradoras; sin embargo todas las organizaciones están expuestas y corren riesgos independientemente del giro, ya que pueden robar sus bases de datos y sistemas con información confidencial o que esta sea encriptada o borrada; además existe el riesgo de fraudes por internet como la clonación de tarjetas. Cabe señalar que este tipo de delito va de la mano con el crecimiento de las compras en línea (CONDUSEF, s.f.).

Por lo anterior es importante que el administrador de la organización analice ciertas variables para contratar al Hacker ético y lo pueda implementar de manera exitosa en su organización; una de las variables a considerar es la de conocimiento que se refiere a los conocimientos adquiridos por estudios así como la experiencia adquirida, una segunda variable son los recursos que incluye los costos e infraestructura necesaria para llevar a cabo dicha actividad, la tercer variable es la ética del Hacker para asegurar la privacidad y la confidencialidad de la información, la cuarta variable es el compromiso de la administración de la organización, que se refiere a la convicción para dar apoyo, seguimiento y tomar acción de los resultados obtenidos del análisis que haya realizado el Hacker ético.

2.2. Conocimientos y experiencia.

En la descripción para contratar a un Hacker ético se encuentra que "puede ser aquel especialista en programación y tecnologías de la información o Ingeniero en Sistemas e Informática pero que tenga la convicción de utilizar su conocimiento para realizar acciones éticas" (El Financiero, 2018).

El perfil del Hacker o Pentester debe ser un profesional con experiencia en hacking, además de contar con certificaciones importantes, entre ellas se encuentran: CISM, CISA, CISSP, SANS, EC-COUNCIL; son profesionales de éxito en el área de seguridad de la información. Además deben de contar con habilidades blandas como el trabajo en equipo y el interés permanente por el aprendizaje (Gacharná, 2009). Hoy en día se busca que un Pentester o Hacker sea experto en programación, "ya que la seguridad informática ha ido variando con el paso del tiempo desde las redes hacia las aplicaciones". Se recomienda que tenga "bases sólidas de programación complementada con redes y firewall" (Parodi, 2018).

Para Muñoz y Sánchez (2017), el Hacker debe contar con: dominio de programación, conocimiento de sistemas operativos como Windows, Unix y Linux, conocimiento de redes y telecomunicaciones, protocolos del servidor web, configuración y gestión telemática e instalación de hardware. Otro requisito a parte de lo descrito con anterioridad es el desarrollo intelectual y de habilidades propias, es decir, la competencia individual (Bissett, 2003).

Por otra parte según Rinsen (2014), los negocios no se encuentran preparados para hacer frente a los riesgos informáticos, en parte por la poca preparación en términos de ciberseguridad en las escuelas. Muchos de los especialistas en ciberseguridad con experiencia práctica no son egresados académicos; la mayoría son autodidactas, por lo que también se debe considerar la experiencia empírica del Hacker.

Para Parodi (2018), "es importante ser una persona autodidacta ya que la tecnología avanza tan rápido que debemos estudiar todo el tiempo para estar a la vanguardia tecnológica y comprender las nuevas soluciones a los problemas que están disponibles en el mercado, cómo funcionan y cómo son aplicadas". Por lo tanto también debe considerarse las herramientas tecnológicas e infraestructura necesaria para llevar a cabo dicha actividad.

2.3. Recursos e infraestructura

Un importante paso para contratar a un Hacker ético es definir los principales riesgos informáticos asociados al quehacer de la empresa y su potencial impacto en términos de recursos económicos; ya que los riesgos de seguridad que se detecten pueden

derivar en la obtención de bases de datos, acceso a redes internas, inyección de código malicioso y fraudes (Arriols, citado por El Financiero, 2018). "Para tener éxito es fundamental cambiar la mentalidad de 'si funciona no lo toques' que previene a las empresas de actualizar sus sistemas y cuestionar sus vulnerabilidades". Los procesos de hacking ético ayudan a reconocer los riesgos y acabar con esa falsa y peligrosa sensación de seguridad. Por tanto, tener un Hacker en una empresa puede ser una muy buena inversión.

Para Bissett (2003), el hacking es una actividad artesanal, en la que no se requiere una gran inversión en infraestructura. Sin embargo hay necesidades básicas que deben de ser cubiertas como el internet y el acceso abierto, es decir, el acceso al código fuente del software es una de las condiciones de libertad que permite a los hackers modificar e innovar.

Por lo tanto, el administrador de la organización debe asegurarse que el Hacker tenga a su disposición la infraestructura necesaria, para garantizar que los usuarios autorizados tengan acceso a la información en el momento que se requiera (Hurtado y Mendaño, 2016).

Por otra parte, el Hacker ético debe contar con herramientas propias para su actividad, entre las más utilizadas según Velasco (2019), se encuentran: Aircrackng, WiFi WPS WPA Tester (herramientas para descifrar contraseñas), Cain & Able (herramienta de descifrado por medio de criptoanálisis), Kismet (paquete de detector de intrusos), AirSnort (recupera las claves de cifrado) , NetStumbler (verifica configuraciones de red, encuentra ubicaciones con una red mal configurada o detecta puntos de acceso no autorizados), Airjack (utilizado para comprobar la integridad de nuestra red mediante el mencionado sistema de inyección de paquetes falsos), inSSIDer (es un escáner de redes inalámbricas de código abierto), CoWPAtty (herramienta que utiliza el diccionario de contraseñas para que podamos recuperarla utilizando el SSID), WepAttack (herramienta de código abierto para recuperar claves WEP 802.11).

Otras herramientas que utilizan los expertos son Fingerprinting organizations with collected archives (FOCA) que es una herramienta para encontrar metadatos e información oculta en documentos de Microsoft Office, Open Office y documentos PDF/PS/EPS, Waffit que permite detectar posibles firewall dentro de los servidores web de una empresa, Kali Linux es una distribución de Linux avanzada para pruebas de penetración y auditorías de seguridad, Metasploit, su objetivo es proveer información de las vulnerabilidades de seguridad informática y ayudar a ejecutar las pruebas de intrusión (Ruales, 2016).

El Hacker debe proporcionar al administrador un informe de los equipos instalados como servidores, programas, sistemas operativos, procedimientos instalados, análisis de seguridad en los equipos y en la red, análisis de la eficiencia de los sistemas y programas informáticos, gestión de los sistemas instalados, verificación del cumplimiento de la Normativa vigente de la Ley Orgánica de Protección de Datos y las vulnerabilidades que pudieran presentarse en una revisión en las estaciones de trabajo, redes de comunicación y servidores (Ruales, 2016). Para asegurar que lo anterior sea conforme a lo establecido en el acuerdo, es importante contemplar la ética del Hacker y sus antecedentes.

2.4. Ética del Hacker

Para poder abordar el tema de ética de un Hacker, primeramente es necesario diferenciar a un Hacker ético y a un Hacker no ético o también denominado delincuente informático. El primero se describe como una persona que realiza ataques a redes en un ambiente controlado y donde la organización ha sido informada, esto con la finalidad de hacerle saber los puntos débiles y el estado de inseguridad de sus redes; mientras el segundo se refiere a aquellas personas que realizan las actividades que hace el Hacking ético pero con la finalidad de servir a organizaciones que realizan acciones fraudulentas (Gacharná, 2009).

Para poder disminuir el riesgo referente a la seguridad de la información y a la privacidad es necesario considerar la ética del Hacker que se va a contratar. La ética del Hacker se considera una nueva moral (Himanen, 2002). La confidencialidad debe ser tal que pueda garantizar que únicamente las personas autorizadas puedan tener acceso a la información; además contar con integridad para cerciorar que la información no ha sido adulterada y así garantizar la integridad de la misma. Así mismo se debe proteger la autenticidad que certifique el origen de la información y su protección para reducir las probabilidades de una situación inesperada aplicando controles (Hurtado y Mendaño, 2016).

Según Enter.co (2014), para que este tipo de intromisiones tenga efecto es necesario que haya consciencia de toda la organización de la importancia de la seguridad de la información, por

lo que se deben instaurar diferentes políticas de seguridad que involucren a todos los actores de la empresa para así poder reducir el nivel de vulnerabilidad.

Para hacerlo el empresario debe generar un proceso de filtros con la intención de tener un elemento seguro como la firma de acuerdos de confidencialidad, ya que en caso de que la relación laboral no sea exitosa podrían quedar en una situación riesgosa (El financiero, 2018). Se debe firmar un contrato donde se absuelva al Hacker ético de toda responsabilidad como consecuencia de las pruebas que realice, siempre que sea dentro del marco acordado (Astudillo, 2013; citado por Ruales, 2016).

El Hacker ético es aquella que da prioridad a sus principios éticos y normas morales, aplica sus conocimientos con fines legales y defensivos, guiándose en los principios de seguridad de las tecnologías de la información que debe garantizar, como: confidencialidad, autenticidad, integridad y disponibilidad (Muñoz & Sánchez, 2017).

Los servicios contratados por las organizaciones se realizan mediante procedimientos controlados y por parámetros de seguridad a fin de asegurar un debido procedimiento y donde no se vea afectada la integridad de su información. “Es así que se realiza esta actividad bajo autorización escrita y bajo protocolos de confidencialidad” (Vidal, 2017). El hacking ético no es un proceso que termine, es continuo e incremental; por lo que se debe dar seguimiento a las recomendaciones hechas por los expertos; para esto se requiere el compromiso por parte de la administración de la organización.

2.5. Compromiso de la administración

El justificar la realización de actividades como el hacking ético a la alta gerencia es una tarea compleja pero fundamental. Según Díaz (2017), la empresa Rapid7 indica que usualmente los departamentos de Tecnologías de información reciben una negativa cuando solicitan realizar este tipo de actividades. Es por esto que es fundamental para los administradores o clientes entender qué es lo que deben recibir y qué es lo que podrán hacer con los reportes y documentos que recibirán.

A los Gerentes y Oficiales de seguridad de las tecnologías de la información de las empresas se les considera los administradores del proyecto y estos son parte fundamental para la implementación del Hacking, ya que la seguridad de los activos de información de una organización son responsabilidad de estos cargos. Estos profesionales son responsables de que la información de la compañía, uno de sus activos más importantes, permanezca integra, confidencial y disponible durante todo su ciclo de vida (Díaz Lira, 2017).

El administrador de proyectos es la persona que tiene la responsabilidad global en un proyecto para que el inicio, la planeación, el diseño, la ejecución, la revisión, el control y el cierre sean exitosos; es el responsable de tomar decisiones y es quien debe asegurarse de controlar el riesgo y minimizar la incertidumbre; además de predecir los problemas potenciales, pensando en soluciones para resolverlos, así mismo debe determinar e implementar las necesidades exactas del proyecto basándose en el conocimiento de la organización (Lledó & Rivarola, 2007).

Por tanto, otra de las variables consideradas para la implementación del hacking ético en una organización, es el compromiso del administrador, el cual debe estar convencido de la utilidad de dicha actividad, ya que debe proveer al Hacker ético con la información necesaria de la organización para que este pueda realizar su trabajo (Astudillo, 2013; citado por Ruales, 2016).

Para el administrador la ejecución del hacking ético debe representar un proyecto, en el cual su desarrollo se ve como una contribución a las metas de la empresa y que justifique con creces su costo. Por lo que el liderazgo es imprescindible para la ejecución del hacking, en donde pueda lograr la participación del personal de modo activo, asegurando que todos conozcan su papel, se sientan capacitados y que conozcan los roles de otros miembros del equipo para lograr un trabajo exitoso (Giannone, Martins, Amatriain, Rodríguez & Merlino, 2018).

El administrador tiene un rol muy importante ya que es quien define y comunica los objetivos y el alcance del proyecto, que estos sean claros, útiles y alcanzables, gestiona los requerimientos del proyecto como equipos, información, acuerdos, cronograma para cumplir tiempos establecidos, además de administrar el presupuesto.

Por lo tanto, se requiere el compromiso de toda la organización y sobre todo del líder del proyecto y/o administrador de la organización, ya que deberá tomar acción una vez que el Hacker haya identificado las brechas de inseguridad informática y que haga las recomendaciones y

diseñe estrategias y métodos para blindar la información de la organización ante un inminente ataque a sus diferentes sistemas informáticos (Vidal, 2017).

3. MÉTODO

Según Hernández Sampieri, Fernández y Baptista (2010), "Los estudios descriptivos pretenden medir o recoger información de manera independiente o conjunta sobre los conceptos o las variables"; y el método exploratorio se utiliza "cuando el objetivo es examinar un tema o problema de investigación poco estudiado". Por lo que esta investigación es del tipo descriptivo y exploratorio, ya que existe poca información disponible acerca de lo que deben conocer los administradores de una organización para la implementación del Hacking ético.

En esta se desarrolló un instrumento para medir las variables propuestas utilizando el método Delphi. Cabero e Infante (2014), señalan que el método Delphi es uno de los más utilizados para especificar las preguntas de investigación y seleccionar las variables de interés entre otros, ya que es una forma rápida de obtener información por parte de expertos.

Se sometió el instrumento a revisión de 6 expertos del área de sistemas y de tecnologías de información ubicados en el Estado de Nuevo León, acerca de los factores que se deben de considerar para la implementación del hacking ético en una organización. Después del primer contacto con los expertos, en donde se obtuvo su retroalimentación, se hicieron las modificaciones al instrumento y una vez más se envió a los expertos para una última revisión y emisión de comentarios.

Posterior a la modificación del instrumento de acuerdo a la retroalimentación recibida por parte de los expertos, se aplicó un muestreo no probabilístico conformada por profesionales de TI para asegurarnos de que el instrumento era entendible y pertinente para el objeto de estudio.

Lo anterior para contestar la pregunta de investigación propuesta:

¿Cuáles son los factores que impactan de manera positiva en la implementación del servicio de hacking ético en las organizaciones?

Se tienen las siguientes hipótesis:

H1: El conocimiento y experiencia impactan de manera positiva en la implementación del servicio de hacking ético.

H2: Los recursos e infraestructura impactan de manera positiva en la implementación del servicio de hacking ético.

H3: La ética del Hacker impacta de manera positiva en la implementación del servicio de hacking ético.

H4: El compromiso de la administración impacta de manera positiva en la implementación del servicio de hacking ético.

En el marco teórico se identifican las variables independientes y la variable dependiente, en donde la variable dependiente se define como la implementación del hacking ético y como variables independientes se proponen el conocimiento y experiencia, los recursos e infraestructura, la ética del Hacker y el compromiso de la administración. A continuación, en la figura 1, se presenta el modelo causa efecto de los factores que impactan de manera positiva en la implementación del hacking ético en las organizaciones.

Figura 1. Modelo propuesto.

Fuente: Elaboración propia

El modelo anterior muestra las variables independientes y dependientes, para esto se desarrolló un instrumento para hacer la medición de las mismas y se aplicó un muestreo no probabilístico a 6 profesionales de TI.

En la primera etapa de evaluación del instrumento con expertos utilizando el método Delphi se obtuvieron algunas observaciones, las cuales fueron tomadas en consideración para hacer las modificaciones siguientes:

Una de las preguntas desarrolladas en el instrumento inicial fue acerca de las certificaciones con las que debe contar el Hacker ético. En la pregunta original se especificaban algunas certificaciones como CISM, CISA, CISSP, SNAS, EC-COUNCIL; se hizo la observación de que no solo existen dichas certificaciones válidas para realizar actividades de hacking, por lo que nos comentaron que esa pregunta se debe de dejar abierta a cualquier tipo de certificación relacionada a la actividad.

En otra aseveración referente a que el Hacker ético debe de contar con dominio en programación, los expertos mencionaron que solo se necesitaban conocimientos básicos, no un dominio total, por lo que se modificó la pregunta, de tener conocimientos básicos en programación y se eliminó la palabra dominio. Así mismo, en otra pregunta acerca de los conocimientos en sistemas operativos que debe tener un Hacker ético, en el instrumento solo se mencionaban sistemas Windows, Unix y Linux, la observación fue agregar el sistema MacOS.

También se había propuesto en el instrumento inicial el prestigio que debe de tener la compañía que ofrece el servicio de hacking ético. Los expertos mencionaron que no solo las empresas de sistemas grandes o reconocidos son las únicas que pueden realizar un buen trabajo de hacking; comentaron que existen pequeñas y medianas empresas que pueden ofrecer el mismo servicio, por lo cual esa pregunta fue eliminada.

Además, en el instrumento inicial, se consideraba una pregunta acerca de las herramientas utilizadas por el Hacker ético, si estas deben ser proporcionadas por la empresa; los expertos consideraron que no era necesaria, ya que todos o la mayoría de los Hackers trabajan con sus propias herramientas.

Así mismo, la pregunta acerca de si consideran que para realizar su trabajo el Hacker ético debe contar con softwares como: Aircracking, AirSnort, entre otras, los expertos consideraron que no se debe contemplar esa pregunta ya que limita los softwares que el Hacker puede utilizar, por lo que también fue eliminada.

Para finalizar la primera revisión por parte de los expertos, se hizo la observación acerca de si consideran que el administrador de la organización debe ser el líder en la implementación del hacking; estos mencionaron que no necesariamente, que era suficiente solo con el hecho de estar convencido de los beneficios del trabajo a realizar para poder tener el acceso y apoyo necesarios, pero no como guía de la actividad y procesos que realiza el hacking ético

Después de hacer las modificaciones que se mencionaron con anterioridad al instrumento, se realizó nuevamente una segunda revisión con expertos, en la cual solo se recibió una observación referente a si consideraban complicado que las organizaciones otorguen el acceso abierto a un

Hacker ético; mencionaron que esa pregunta no era necesaria ya que el acceso depende del alcance del proyecto y eso se establece desde el inicio de este; por lo cual se eliminó esa pregunta. En resumen, de 30 preguntas que se tenían contempladas en el instrumento inicial con las dos revisiones por parte de los expertos, quedaron un total de 25.

Posteriormente se aplicó el instrumento final a una muestra no probabilística para confirmar si el objetivo estaba claro.

En el rango de respuesta se utiliza una escala Likert de cinco opciones para todas las preguntas:

1	2	3	4	5
Totalmente de acuerdo	Parcialmente de acuerdo	Ni de acuerdo ni en desacuerdo	Parcialmente en desacuerdo	Totalmente en desacuerdo

4. RESULTADOS

Los resultados obtenidos se muestran en las siguientes tablas:

Tabla 1. Variable independiente conocimiento y experiencia

		1	2	3	4	5
1.-	Considera que el Hacker ético debe contar con carrera profesional.	33%	50 %	0%	0%	17 %
2.-	Considera que el Hacker ético debe contar con una Certificación profesional.	83%	17 %	0%	0%	0%
3.-	Considera que el Hacker ético debe contar con experiencia comprobable en otras organizaciones.	67%	33 %	0%	0%	0%
4.-	Considera que el Hacker ético debe contar con habilidades blandas como: trabajo en equipo y capacidad de análisis.	67%	0%	17 %	0%	17 %
5.-	Considera que el Hacker ético debe contar con conocimientos adquiridos de forma empírica.	67%	33 %	0%	0%	0%
6.-	Considera que el Hacker ético debe contar con conocimientos básicos en programación.	83%	17 %	0%	0%	0%
7.-	Considera que el Hacker ético debe contar con conocimientos en los sistemas operativos: Windows, Unix, Linux y MacOS.	83%	17 %	0%	0%	0%
8.-	Considera que el Hacker ético debe contar con conocimiento en redes.	100 %	0%	0%	0%	0%
9.-	Considera que el Hacker ético debe contar con dominio en protocolos del servidor web y configuración.	100 %	0%	0%	0%	0%
10.-	Considera que el Hacker ético debe contar con dominio en gestión telemática e instalación de hardware.	33%	17 %	33 %	17%	0%

Fuente: Elaboración propia

En promedio se obtuvo como resultado que el 72% de los expertos está totalmente de acuerdo con las aseveraciones realizadas para la variable de conocimiento y experiencia, el 18% parcialmente de acuerdo, el 5% ni de acuerdo ni en desacuerdo, el 2% parcialmente en desacuerdo y el 3% totalmente en desacuerdo. Con esta información podemos concluir que la hipótesis 1 se acepta; es decir, que el conocimiento y experiencia si impactan de manera positiva en la implementación del servicio de hacking ético.

Tabla 2. Variable independiente recursos e infraestructura

		1	2	3	4	5
17. -	Considera que el Hacker debe contar con sus propias herramientas de software y hardware.	50%	33 %	17 %	0%	0%
18. -	Considera que las herramientas que utiliza el Hacker ético deben ser las más utilizadas en el mundo del Hacking.	33%	0%	33 %	33%	0%
19. -	Considera que las herramientas utilizadas por el Hacker ético deben ser controladas por la organización.	50%	0%	17 %	17%	17 %
20. -	Considera justificable costo-beneficio la contratación del servicio de Hacking ético.	100 %	0%	0%	0%	0%
21. -	Considera que las organizaciones están dispuestas a pagar lo necesario para garantizar la seguridad de su información.	17%	33 %	17 %	33%	0%

Fuente: Elaboración propia

Para la segunda variable recursos e infraestructura se obtuvo como resultado que el 50% está totalmente de acuerdo con las aseveraciones, el 13% parcialmente de acuerdo, el 17% ni de acuerdo ni en desacuerdo, el 17% parcialmente en desacuerdo y el 3% totalmente en desacuerdo. Con esta información podemos concluir que la hipótesis 2 se acepta; es decir, que los recursos e infraestructura si impactan de manera positiva en la implementación del servicio de hacking ético.

Tabla 3. Variable independiente ética del Hacker

		1	2	3	4	5
11. -	Considera que el servicio de Hacking ético debe ser mediante un contrato de confidencialidad.	83%	17 %	0%	0%	0%
12. -	Considera que el Hacker ético no debe tener experiencia en ataques no éticos.	17%	0%	67 %	0%	17 %
13. -	Considera que la privacidad de la información de la organización debe ser protegida.	100 %	0%	0%	0%	0%
14. -	Considera que uno de los principios de seguridad para un Hacker ético es mantener la integridad de la información de la organización.	67%	17 %	17 %	0%	0%
15. -	Considera que uno de los principios de seguridad para un Hacker ético es mantener la autenticidad de la información de la organización.	83%	17 %	0%	0%	0%
16. -	Considera que uno de los principios de seguridad para un Hacker ético es mantener la disponibilidad de la información de la organización.	83%	0%	17 %	0%	0%

Fuente: Elaboración propia

Para la tercera variable la ética del Hacker se obtuvo como resultado que el 72% está totalmente de acuerdo con las aseveraciones, el 8% parcialmente de acuerdo, el 17% ni de acuerdo ni

en desacuerdo, el 0% parcialmente en desacuerdo y el 3% totalmente en desacuerdo. Con esta información podemos concluir que la hipótesis 3 se acepta; es decir, que la ética del Hacker si impacta de manera positiva en la implementación del servicio de hacking ético.

Tabla 4. Variable independiente compromiso de la administración

		1	2	3	4	5
22.-	Considera que el encargado de sistemas como líder del proyecto debe dar seguimiento a las recomendaciones realizadas por el Hacker ético.	67%	17%	17%	0%	0%
23.-	Considera que el administrador de la organización debe brindar el apoyo necesario para realizar el Hacking ético.	100%	0%	0%	0%	0%
24.-	Considera que el administrador de la organización debe estar convencido de los beneficios que trae consigo la aplicación del Hacking ético.	100%	0%	0%	0%	0%
25.-	Considera que el administrador de la organización debe comunicar al resto de los empleados los beneficios que se pueden lograr al implementar el Hacking ético.	67%	17%	17%	0%	0%

Fuente: Elaboración propia

Para la cuarta variable el compromiso de la administración de la organización se obtuvo como resultado que el 83% está totalmente de acuerdo con las aseveraciones propuestas, el 8% parcialmente de acuerdo, el 8% ni de acuerdo ni en desacuerdo, el 0% parcialmente en desacuerdo y el 0% totalmente en desacuerdo. Con esta información podemos concluir que la hipótesis 4 se acepta; es decir, que el compromiso de la administración si impacta de manera positiva en la implementación del servicio de hacking ético.

5. CONCLUSIONES

En esta investigación podemos concluir que se observan algunas diferencias entre los resultados obtenidos y lo que opinan algunos autores; uno de los puntos es que la mayoría de los expertos consideran que no es necesaria una carrera profesional para realizar actividades de hacking; le dan mayor valor al aprendizaje empírico, además de que consideran que no es tan necesario contar con dominio en gestión telemática e instalación de hardware a diferencia de lo que se investigó en otros artículos.

Otro punto es que los expertos que se entrevistaron en esta investigación consideran poco importante que el Hacker ético no tenga antecedentes en ataques no éticos; contrario a lo que nos marcan diversas investigaciones acerca de la ética del Hacker. Además difícilmente se puede identificar quién ha tenido este tipo de prácticas, ya que es información que generalmente no se agrega a un curriculum vitae.

Así mismo los expertos consideran que no es necesario contar con las herramientas más utilizadas en el mundo del Hacking; a diferencia de algunos autores que lo recomiendan. Otro punto es que según los expertos, las organizaciones en la mayoría de los casos no siempre están dispuestas a pagar lo necesario para proteger su información, por lo que no es tan sencillo lograr una actitud positiva y el compromiso por parte de la administración de la organización donde se brinda el servicio.

Sin embargo para poder obtener información a mayor escala acerca de la actividad del hacking ético y de las variables que se deben considerar para su aplicación exitosa en una organización, se tiene como proyecto una siguiente investigación, en donde este instrumento será aplicado a una muestra representativa de expertos de TI que dan servicio a las organizaciones en el área metropolitana de la ciudad de Monterrey, para conocer su percepción acerca de las variables propuestas en la investigación presente.

REFERENCIAS

Bissett, A., (2003). Hacker ethics in the marketplace: the example of freeware. *Journal of Information, Communication and Ethics in Society. 1*(1), 31-38. https://doi.org/10.1108/14779960380000224

Cabero, J., e Infante, A. (2014). Empleo del método Delphi y su empleo en la investigación en Comunicación y Educación. EDUTEC *Revista Electrónica de Investigación Educativa, 48,* 1-16. Recuperado de: http://edutec.rediris.es/Revelec2/Revelec48/pdf/Edutec- e_n48_Cabero-Infante.pdf

CONDUSEF. (s.f.). *Condusef estadística*s. Recuperado de https://www.condusef.gob.mx/gbmx/?p=estadisticas

Díaz, M. A., (2017). *Framework para la entrega de Reportes de Test de Penetración a Aplicaciones Web* (tesis de pregrado). Universidad Técnica Federico Santa María, Chile.

Enter.co. (2014). *Enter.co*. Recuperado de: https://www.enter.co/guias/tecnoguias-para-empresas/que-es-el-hacking-etico-y-por-que-es-necesario/

Gacharná G., F. (2009). Hacker ético vs delincuente informático: Una mirada en el contexto colombiano. *INVENTUM, 4*(6), 46-49. doi.org/10.26620/uniminuto.inventum.4.6.2009.46-49

Giannone, A., Martins, S., Amatriain, H. G., Rodríguez, D., & Merlino, H. (2018). Inclusión de hacking ético en el proceso de testing de software. In *XX Workshop de Investigadores en Ciencias de la Computación (WICC 2018, Universidad Nacional del Nordeste).*

Gil, V., & Gil, J. (2017). Seguridad informática organizacional: un modelo de simulación basado en dinámica de sistemas. *Scientia Et Technica*, *22* (2), 193-197.

Gómez A. V. (2014) *Tipos de ataques y de intrusos en las redes informáticas*. Recolectado de http://www.edisa.com/wp-content/uploads/2014/08/Ponencia_Tipos_de_ataques_y_de_intrusos_en_las_redes_informaticas.pdf. Marzo 2018.

Guevara, A. (7 junio de 2012). El hacking ético y la seguridad de la información de empresas en México - parte ii. *Revista Seguridad*, *13*(31). Recuperado de https://revista.seguridad.unam.mx/numero-13/el-hacking-%C3%A9tico-y-la-seguridad-de-la-informaci%C3%B3n-de-empresas-en-m%C3%A9xico-parte-ii

Hernández, R., Fernández, C., & Baptista, P. (2010). *Metodología de la investigación*. México: McGraw-Hill.

Himanen, P. (2002). *La ética del hacker y el espíritu de la era de la información.*, UNSPECIFIED. [Book]

Hurtado, M., & Mendaño, L. (2016). Implementación de técnicas de hacking ético para el descubrimiento y evaluación de vulnerabilidades de la red de una cartera de Estado. Ecuador: Quito

Johansen, R. (March 4, 2017). *Ethical Hacking Code of Ethics: Security, Risk & Issues*. EUA: Panmore Institute. Recuperado de: http://panmore.com/ethical-hacking-code-of-ethics-security-risk-issues

Lledó, P., & Rivarola, G. (2007). *Gestión de proyectos*. Buenos Aires, Argentina: Pearson Educación.

Muñoz, A., & Sánchez, J. (2017). *Modelo referencial de aprendizaje para la implementación de Hacking ético* (trabajo de grado). Universidad Libre de Colombia, Bogotá.

Ortega, O. (11 de abril de 2018). ¿Un hacker para tu empresa? Podría ser una buena idea. *El Financiero*. Recuperado de: https://www.elfinanciero.com.mx/tech/un-hacker-para-tu-empresa-podria-ser-una-buena-idea

Parodi, A. (2018). *¿Qué conocimientos necesita tener un buen hacker?* Quora. Recuperado de https://es.quora.com/Qué-conocimientos-necesita-tener-un-buen-hacker

Pixel, M. (2018). *Con más de un millón de casos en 2018, los fraudes cibernéticos ya superaron a las estafas y clonaciones de tarjetas en México*. México: Xataka. Recuperado de https://www.xataka.com.mx/seguridad/millon-casos-2018-fraudes-ciberneticos-superaron-estafas-clonaciones-tarjetas-mexico

Risen, T. (2014). Not Prepared for Hacks. U.S. *News Digital Weekly*, *6*(22), 8. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,url,uid,cookie&db=a9h&AN=96273523&lang=es&site=ehost-live

Rodríguez, E. R. (2016). *Proceso de auditoría interna y Ethical* Universidad Piloto de Colombia).

Ruales, C., (2016). *Auditoría de Seguridad Perimetral en Dispositivos de capa 3 para entornos empresariales utilizando la herramienta Kali Linux* (tesis de doctoral), Universidad de Guayaquil Facultad de Ciencias Matemáticas y Físicas Carrera de Ingeniería en Networking y Telecomunicaciones, Ecuador.

Saavedra, M., & Tapia, B. (2013). El uso de las tecnologías de información y comunicación TIC en las micro, pequeñas y medianas empresas (MIPyME) industriales mexicanas, *Revista Venezolana de Información, Tecnología y Conocimiento, 10*(1), 85-104.

Stephen, L. (2000) "Information technology in business processes". *Business Process Management Journal,* 6(3), pp.224-237. doi.org/10.1108/14637150010325444.

Velasco, R. (2019). *Las mejores herramientas para hacking ético y analizar redes Wi-fi*. Softzone. Recuperado de:https://www.softzone.es/2018/01/12/mejores-herramientas-hacking-etico-2018/

Vidal, J. H. (2017). *Una nueva experiencia en seguridad hacking ético*. (Trabajo de grado). Universidad Militar Nueva Granada, Colombia.