Marcelo León
Universidad Tecnológica Empresarial de Guayaquil, Ecuador.
marcelo.leon@unileon.es
https://orcid.org/ 0000-0001-6303-6615

Paulina León
Universidad Tecnológica Empresarial de Guayaquil, Ecuador.
paulinaleon07@yahoo.es
https://orcid.org/ 0000-0003-3271-4019

Recibido: 2020- 11- 15 | Revisado: 2020-12-14
Aceptado: 2021- 01- 10 | Publicado: 2021-01-19

Hacking ético en el sector financiero

Ethical hacking in the financial sector

RESUMEN

En el presente artículo se analizará sobre los beneficios que brindan el hacking ético en las instituciones bancarias, también se evaluará sobre la seguridad de la información que poseen las entidades financieras, ya que en la actualidad son las principales víctimas de ataques informáticos. Por lo tanto, se considera necesario que toda institución financiera debe poseer una seguridad informática, validada por las diferentes normas de seguridad y garantizada por un hacker ético, ya que es la persona que desarrolla su propia herramienta para trabajar, brindando un mejor servicio a las entidades financiera. Para poder contar con un hacking ético es necesario tener el permiso de la compañía, evitando problemas a futuro, es necesario realizar un contrato de confiabilidad, indicando cuales son las responsabilidades que se debe de cumplir, exponiendo los beneficios en las instituciones financieras al momento de contar con un hacking ético, ya que se busca evitar las vulnerabilidades de las entidades financieras.

Palabras claves: hacking ético, entidades financieras, seguridad informática.

Abstract: In this article we analyze the benefits of ethical hacking in banking institutions, it also evaluates the security of information that is related to financial institutions, which are currently the main causes of computer attacks. Therefore, you have to take into account that this in its entirety must be in a computer security, a validation by the different security standards and guaranteed by an ethical hacker, and that is the person who has his own tool to work, providing a better service to financial institutions. In order to have a hacking, it is necessary to have the company's permission, avoiding problems in the future, it is necessary to make a reliability contract, indicating which are the responsibilities that you must fulfill. Exposing the benefits in financial institutions at the time of having an ethical hacking, which seeks to avoid the vulnerabilities of financial institutions.

Keywords: ethical hacking, financial entities, computer security.

1. INTRODUCCIÓN

Hoy en día los hackers son muy comunes y existen en las diferentes partes del mundo perjudicando a las diferentes entidades, sean públicas o privadas, los hackers obtienen la información de manera ilegal para hacer daño a las transacciones de las personas y de las entidades financieras. Sus principales objetivos son los sectores financieros y los gobiernos (DC, 2016). Con el avance de las tecnologías en la actualidad las empresas tienen mayor riesgo de ser hackeadas de manera fácil y rápida y pueden además, robar su información. Por tal motivo se considera que las empresas deben de contratar a un personal de hacking ético para que se les pueda brindar una buena seguridad a toda su información y evitar el robo de datos.

Las nuevas tecnologías de la información están presentes en las operaciones de transacciones financieras vía internet y varios beneficios que brindan las entidades. Las aplicaciones móviles también corresponden al nuevo auge de beneficios que tienen a disposición los usuarios. Por lo tanto, dado el caso obliga a los sistemas o aplicaciones informáticas, contar con un máximo nivel de seguridad para la empresa que genera los datos y los usuarios que accede a las transacciones (Burgos Rivera, 2016).

De esta manera se dará el cumplimiento de normas que rigen para la protección de información que se establece legalmente para cada región. Para dar mejora a la seguridad de las entidades financieras se crea una solución apropiada al problema, las organizaciones financieras visualizaron que la mejor solución es determinar y evaluar todas clases de amenazas, por lo cual se debe contar con personas profesionales en seguridad informática y *ethical hacking* para que intenten evadir las amenazas en sus sistemas informáticos financieros. Las instituciones más vulnerables a estos ataques cibernéticos considerándose su importancia y relevancia para el desarrollo económico de las naciones son precisamente las entidades financieras (Gavilánez & Zambrano, 2017).

1. Hacking ético

El hacking ético es considerado por una persona capaz de comprobar si existe la vulnerabilidad y se encarga de la seguridad en la empresa en sus datos, para después de un análisis adecuado poder presentar un informe de como esta la seguridad de la empresa y así poder revelar si existe algún fallo de seguridad y poder llegar a una solución rápida sin que afecte a la institución y evitando que la información de la empresa sea atacada por personas mal intencionadas.

Se considera a una persona como un hacker ético cuando ayuda a cuidar con la seguridad de la empresa y tiene mucho cuidado con la seguridad, también sobreguarda todas las informaciones de las instituciones. Evalúa la seguridad e identifica vulnerabilidades en sistemas, redes o infraestructura de sistemas, esto incluye encontrar y explotar algunas vulnerabilidades para determinar cuándo hay acceso sin autorización u otras actividades maliciosas (Avila, 2019).

Se considerada como pruebas de penetración a las respuestas que se realizaron tiempos atrás a

N° 15, Vol 8 - enero 2021
ISSN: 1390-9045
e-ISSN: 2602-8190

los primeros ataques informáticos, por lo que ese tiempo se consideró importante ya que tuvo grandes consecuencias como es perdida de ingresos monetarios a la empresa y la reputación de la institución. Es aquí en donde es de mucha importancia que toda institución financiera obtenga un hacker ético ya que una de sus principales labores es poder buscar las vulnerabilidades en los sistemas que posee las instituciones financieras para así poder evitar la fuga de información que solo tiene interés en la institución (Soriano, 2018).

2. TIPOS DE HACKERS

Existen dos tipos de hackers principales: los Black Hat y los White Hat. Sus nombres provienen de películas donde hay buenos y malos, normalmente, a "los malos" se le conoce como sombreros negros y los "los buenos" se lo conoce como los de sombrero blanco. A continuación, se detalla los tipos de hackers (Figura1).

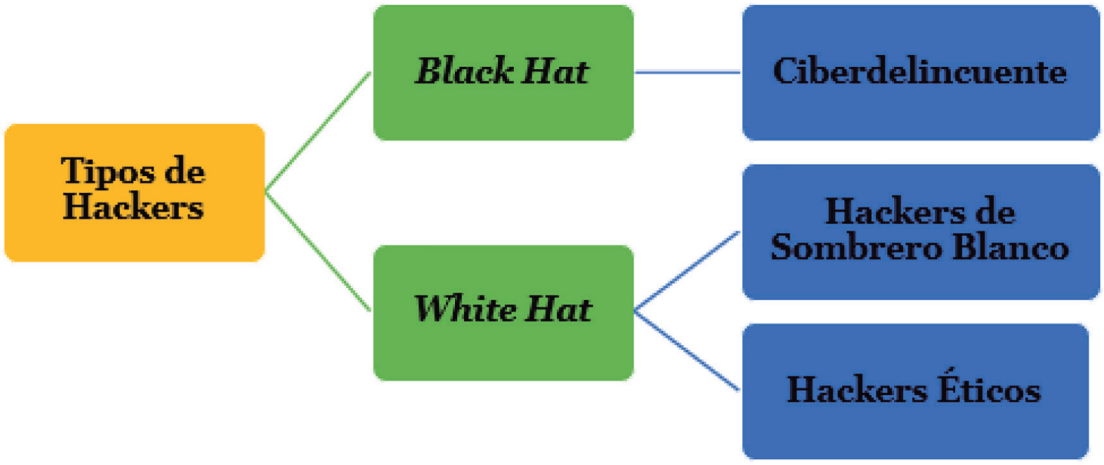

Figura 1 – Tipos de Hackers

2.1. Black Hat

Son aquellos que se les considera como sombrero negro y ellos se dedican a realizar actividades ilícitas para así poder extraer toda la información confidencial de la empresa, este tipo de personas se encargan de crear software tipo malware que perjudican a las instituciones que no tengan una buena seguridad.

Esto es lo que puede hacer un hacker:

- **Reconocimiento:** El hacker hace el reconocimiento pasivo previo a cualquier ataque, recopila información sobre el objetivo a atacar para poder llegar a obtener información.
- **Escaneo:** Se escanean los diferentes medios por donde se puede hacer el ataque, como por ejemplo la red, pero esta se realiza ya con información de la fase previa.

- **Obtener acceso:** Obtención de acceso, se refiere al ataque propiamente dicho, por ejemplo, hacer uso de un exploit o bug, para obtener una contraseña.
- **Mantener acceso:** se trata de seguir tendiendo los privilegios obtenidos.
- **Borrado de evidencia:** Borrar las evidencias con lo que pueda ser descubierto (Sandra, 2017).

2.2. White Hats

Este tipo de personas es de aquellos que se encargan de encontrar la vulnerabilidad que posee un sistema y así poder corregir fallos que se presenten y ahora se considera como una de las personas importantes para las instituciones ya que con sus conocimientos mejoran con la seguridad de las empresas (Muñez, 2015).

Hoy en día a las empresas le resulta beneficioso contar con los conocimientos y servicios de un hacker ético. Independientemente del tamaño de la empresa es decir sea grande o pequeña la empresa, debe de proteger su seguridad de una forma correcta (RD, 2018).

3. IMPLEMENTAR EL HACKING ÉTICO EN SISTEMAS FINANCIEROS

El hacking ético financiero es la capacidad de brindar una medida de seguridad, a su vez es conocido por revisar y verificar muchos aspectos de sistemas financieros y proteger la información de los clientes.

La misión de un hacker ético es implementar esta tecnología y seguir protocolos de seguridad, detectando las vulnerabilidades que se generan en el sistema financiero. La implementación del hacking ético en casos financieros es determinar y diagnosticar los servicios que pueden recibir ataques informáticos y caer en un riesgo de robar información y dinero de manera electrónica. Las metodologías de hacking ético, representan una fotografía al estado de la ciberseguridad de una organización en un determinado tiempo (Andrés, 2017).

La solución que se brinda a los usuarios de las entidades financieras es netamente importante ya que una vez que se corrige las vulnerabilidades, se debe dar el debido mantenimiento de la seguridad del sistema ya que ocurren actualizaciones de los sistemas financieros a diario (Arturo, 2015).

3.1. Importancia de la información para las organizaciones

Se ha considerado que todas las organizaciones, están compuestas por un conjunto de procesos que hace que se comuniquen entre si a través de intercambio de informaciones, ya que la comunicación es el activo más importante de todas las empresas en la actualidad; por lo tanto, es importante que todas las organizaciones tengan toda su información respaldada y segura para evitar el robo de datos, se ha considerado que la seguridad de la información depende de que la empresa garantice sus principios fundamentales como son: la confidencialidad, la integridad y la disponibilidad (Enrique & Sanches Allende, 2017).

N° 15, Vol 8 - enero 2021
ISSN: 1390-9045
e-ISSN: 2602-8190

3.2. Elementos esenciales de la seguridad:

- **Confidencialidad:** tiene que ver con la ocultación de información o recursos.
- **Autenticidad:** es la identificación y garantía del origen de la información.
- **Integridad:** se refiere a cambios no autorizados en los datos.
- **Disponibilidad:** posibilidad de hacer uso de la información y recursos deseados (Solano, 2011).

4. ¿QUÉ EVALÚA UN HACKER ÉTICO?

Es aquel que evalúa los servicios que ofrecen los hackers blancos, por lo tanto, las empresas son considerados como pruebas de penetración, con el objetivo de analizar que las empresas estén bien protegidas por algún ataque mal intencionado por personas externas y puedan ingresar al sistema de la empresa por medio de la red. A continuación se presenta (Figura 2) donde muestra las ventajas principales que posee un Hacking Ético.

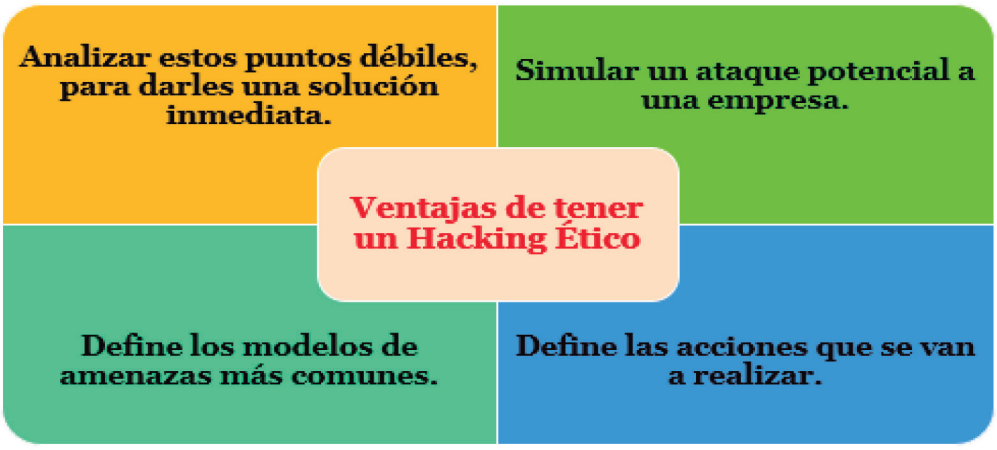

Figura 2 – Ventaja de un Hacking ético

Se ha demostrado que la mayoría de los hackers están motivados por la curiosidad de conocer nuevas herramientas para obtener información, por lo tanto, ellos crean nuevos programas que permiten el ingreso a cualquier empresa, teniendo como uno de su principal desafío encontrar la forma de evitar el robo de información. Si una persona quiere convertirse en un hacking ético o conocido también como sombrero blanco, lo puede realizar preparándose a menudo con las nuevas tecnologías que existen en la actualidad y puede ayudar a empresas a evitar que le roben su información.

Se ha considerado que la protección de los sistemas en la actualidad requiere de un amplio conocimiento de personas especializadas en este campo, ya que buscan evitar ataques a las instituciones sean estas públicas o privadas. Hoy en día la piratería ética efectiva se lo conoce como un conocimiento de la red de los sistemas, el uso de la piratería cada vez aumenta en instituciones financieras (Freeman, 2016).

5. ACTUALIDAD DEL HACKING ÉTICO

El ethical hacking se ha ido apropiando con gran fuerza a la parte de la seguridad informática, a escala en que las entidades financieras o afines aumentan y la innovación tecnológica crece de muy buena forma, surge así que este término está en un gran repunte y enterarse de que esta práctica está activa a nivel de la informática, se hace obligatorio pretender poner freno a los ataques informáticos y robo de información de las personas.

El hacking ético toma bien su lugar en las organizaciones financieras. A medida que los servicios tecnológicos evolucionan y las transacciones en línea que se realizan por las compras o servicios bancarios, es importante saber que los usuarios cada vez más implementan estos servicios que ofrecen las entidades bancarias para simplificar el tiempo neto que se puede emplear en este tipo de procesos tecnológicos, pero esto acarrea una preferencia del incremento de alteración de la seguridad informática, así como va en crecimiento los ataques denominados *phishing* contra entidades financieras y de esa manera también se implementan nuevas tecnologías de seguridad en las diferentes plataformas virtuales, también restauran y mejoran el trabajo de atacar con herramientas actualizadas y en mayor calidad, queriendo siempre vulnerar la seguridad informática quebrantando contra los pilares fundamentales de la seguridad informática: confidencialidad, integridad y disponibilidad de la información. (Burgos Rivera, 2016).

6. CONCLUSIONES

Resulta importante contar con un hacking ético ya que permite prevenir un robo de información de la empresa por personas mal intencionadas que quieren hacer daño a las instituciones financieras.

Los ataques de seguridad en las entidades financieras, en la actualidad son muy comunes por medio de los hackers, por lo tanto, las empresas están en la obligación de mejorar su seguridad en sus datos.

Es importante que todas las empresas financieras cuenten con un hacking ético para así poder proteger sus datos con mayor seguridad. Teniendo como resultado el mostrar a accionistas, dueños o gerentes de la empresa cuales son las debilidades en seguridad que posee su negocio y así poder mejorarlas.

REFERENCIAS

Andrés, S. M. (2017). *Metodología de hacking ético para instituciones financieras, aplicación de un caso práctico.* Tesis de Maestría, Cuenca.

Arturo, U. L. (2015). *Hacking Ético, detección de vulnerabilidades en sistemas informáticos.* Universidad Piloto de Colombia, Colombia. Obtenido de http://repository.unipiloto.edu.

N° 15, Vol 8 - enero 2021
ISSN: 1390-9045
e-ISSN: 2602-8190

co/bitstream/handle/20.500.12277/2898/00002225.pdf?sequence=1&fbclid=IwAR15fZJf7yhM44lK9G5QKmcLWg7nEUD-Cck5TP7nuZJF8JwuOU-FnUpObus

Avila, M. A. (2019). Hacking etico: Impacto en la Sociedad. Bogotá, Colombia.

Burgos Rivera, D. A. (2016). *La importancia del hacking ético en el sector financiero.* Universidad Piloto de Colombia. Bogota: Universidad Piloto de Colombia. Obtenido de http://polux.unipiloto.edu.co:8080/00003049.pdf

DC. (16 de Febrero de 2016). Segurida:Hackers atacan más a los bancos y gobiernos. (D. E. Comercio, Ed.) *Diario El Comercio*. Obtenido de https://www.elcomercio.com/actualidad/hackers-atacan-bancos-gobiernos-titulos.html

Enrique, J., & Sanches Allende, J. (2017). *Riesgo de Ciberseguridad en las empresas.* Madri.

Freeman, R. (2016). Ethical hacking: what is it, and why would I need it?

Gavilánez, R., & Zambrano, D. (2017). Análisis de los ataques de hackers a entidades financieras: Una revisión post-literaria. *JEM Journal of Economics and Management*, 1-8.

Muñez, A. (31 de 10 de 2015). ¿Qué es un hacker y qué tipos de hacker existen? *ComputerHoy*.

RD. (31 de julio de 2018). *ReporteDigital*. Obtenido de Las ventajas de tener un hacker en el entorno empresarial: https://reportedigital.com/seguridad/ventajas-hacker-entorno-empresarial/

Rivera, D. A. (s.f.). *La importancia del hacking ético en el sector financiero.* Bogotá,Colombia.

Sandra, C. C. (2017). *White hat: Hacking ético.* Tesis de Licenciatura, Universidad Piloto de Colombia, Colombia.

Solano, V. M. (2011). *Hacking y ciberdelito.* niversidad Politécnica de Valencia. Obtenido de https://riunet.upv.es/bitstream/handle/10251/11856/memoria.pdf?sequence=1&isAllowed=y

Soriano, A. G. (2018). Hacking ético: mitos y realidades. *revista.seguridad*(12).