Revisión sobre hacking ético y su relación con la inteligencia artificial

Review on Ethical Hacking and its Relationship with Artificial Intelligence

Javier Andrés Ardila Osma, Eimmy Fernanda Salcedo González,
César Augusto Pedraza Aguirre, Miguel Ángel Saavedra Melo*

Resumen

En el presente documento se realiza la descripción general de las principales características de los procesos de hacking ético como herramienta de seguridad informática aplicando inteligencia artificial (IA) teniendo en cuenta que la adopción de estrategias de protección de información en las organizaciones ya no es un lujo que solo algunas adoptan, sino prácticamente una exigencia teniendo en cuenta la necesidad de contrarrestar riesgos en redes locales y de internet. La IA es un paradigma tecnológico que cada vez es más usado en la industria y las organizaciones como soporte de sus procesos y se ha vuelto tan relevante que negarse a usarla implicará dificultades importantes en el mediano plazo para estar a la altura de las demandas y no quedar relegada del futuro. La estructura del documento se compone de varias secciones, primero se presenta la definición y el origen histórico del hacking y el hacking ético, en seguida se define el concepto de inteligencia artificial y se establece su relación con el hacking ético, sus algoritmos más utilizados y sus ventajas y desventajas; a continuación, se presentan detalles del contexto actual del hacking ético a nivel global y local, así como de su marco regulatorio; después se mencionan las principales vulnerabilidades detectadas el hacking ético, se presentan unas someras recomendaciones y finalmente las conclusiones más relevantes encontradas.

Palabras clave:
Hacking, hacking ético, inteligencia artificial, aprendizaje, malware, marco regulatorio.

Abstract

This document provides an overview of the main characteristics of ethical hacking processes as a computer security tool applying artificial intelligence (AI), taking into account that the adoption of information protection strategies in organizations is no longer a luxury that only some adopt, but practically a requirement that takes into account the need to counteract risks in local networks and the Internet. AI is a technological paradigm that is increasingly used in industry and organizations to support their processes and has become so relevant that refusing

* Fecha de recibido: 13/08/2020 Fecha de aceptación: 18/12/2020
Correo electrónico: 68191512@unitec.edu.co, 68181527@unitec.edu.co, 68131507@unitec.edu.co, miguelsaavedra@unitec.edu.co
Citar como: Ardila Osma, J. A., Salcedo González, E. F., Pedraza Aguirre, C. A., & Saavedra Melo, M. Á. (2020). Revisión sobre hacking ético y su relación con la inteligencia artificial. *Revista RETO, 8.*

to use it will imply significant difficulties in the medium term to keep up with the demands and not stay relegated from the future. The structure of the document is made up of several sections, first the definition and the historical origin of hacking and ethical hacking are presented, then the concept of artificial intelligence and its relationship with ethical hacking, its most used algorithms and its advantages and disadvantages. Disadvantages The current context of ethical hacking at global and local level, as well as its regulatory framework, is detailed below; then the main vulnerabilities detected in ethical hacking are mentioned, brief recommendations are presented and finally the most relevant conclusions are shown.

Keywords:
Hacking, ethical hacking, artificial intelligence, machine learning, malware, regulatory framework.

Introducción

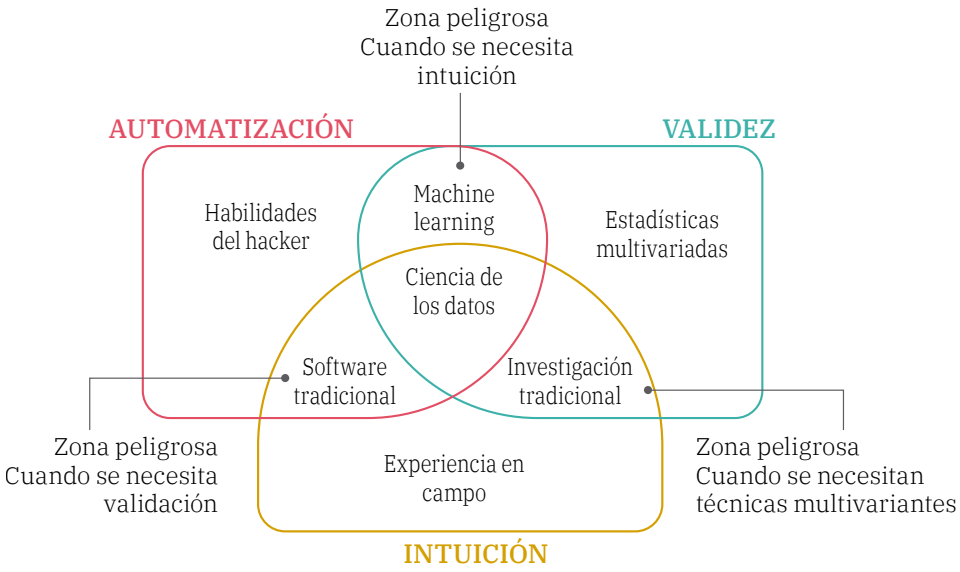
En la actualidad los avances tecnológicos como el almacenamiento de información en la nube y el internet de las cosas (IoT), han abierto una puerta enorme dejando a las organizaciones y las personas propensas a cualquier ataque cibernético. El problema de gestionar y vigilar el riesgo que se presenta en estas áreas de modo efectivo e instantáneo requiere de una pieza primordial: los datos. Estos datos son analizados por sistemas que se han vuelto inoficiosos en escenarios difíciles, como por ejemplo lo ocurrido en el Banco de Chile en 2018 cuando perdió 10 millones de dólares en un robo mientras los encargados de seguridad se ocupaban de atender otro ataque que los mantuvo ocupados (P., 2019). Es vital que en estas situaciones la conjunción de datos se haga de manera más capaz y eficaz. La preferencia en la utilización de la AI en el hallazgo y prevención de asaltos necesita que las organizaciones divulguen esta información de dichos asaltos en el menor tiempo posible para poder mitigar los riesgos. En estos momentos el hombre cuenta con tecnologías que le permiten construir maquinas con programas específicos que permiten identificar las inseguridades del sistema automáticamente. Esto facilita examinar grandes volúmenes de datos y tomar medidas de precaución y protección.

Las compañías que no poseen un historial actual de estos ataques y que no utilizan la AI para detectarlos se encuentran totalmente vulnerables ante estos riesgos. Es sabido que algunas organizaciones realizan sus auditorias en seguridad utilizando una maquina con un software específico, que ha sido entrenada para buscar los riesgos latentes en todo el sistema. La mecanización de los hackers es algo que se está fortaleciendo actualmente y que se lleva a cabo gracias a la implementación de la AI, pero para esto es necesario contar con personas que posean destrezas en investigación, habilidades para realizar algoritmos de entrenamiento, análisis para hallar nuevas amenazas cibernéticas. Así como también maquinas inteligentes diseñadas para automatizar mecanismos protección y defensa. Concisamente, lo anteriormente mencionado puede ser sintetizado en el siguiente diagrama mostrado en la figura 1.

Definición y orígenes del hacking ético

En la actualidad, las compañías manejan grandes volúmenes de datos que necesitan ser vigilados y protegidos para estos que no sean accedidos por usuarios no autorizados, generalmente a través del uso de herramientas de software maliciosas, para ser utilizados de manera ilegal, o ser retenidos con intenciones lucrativas. Para evitar que esto suceda, las personas con amplio conocimiento sistemas, en particular en protocolos de seguridad de redes e internet, y con conocimiento de herramientas como IA, pueden implementar metodologías para la realización de una serie de pruebas que permitan saltar y evitar todas las medidas de seguridad que tiene el sistema de la organización, identificando todas las vulnerabilidades posibles. Estas personas son conocidas como hackers éticos y lo que realizan al final es una auditoría de seguridad con la implementación de procedimientos como penetration test, vulnerability test, o simplemente pentest (Federico Ivan Gacharna 2009), previa autorización de la organización, cuyos resultados se entregan a los encargados del sistema para

Figura 1. Relación entre hacking, aprendizaje de máquina y ciencia de datos.

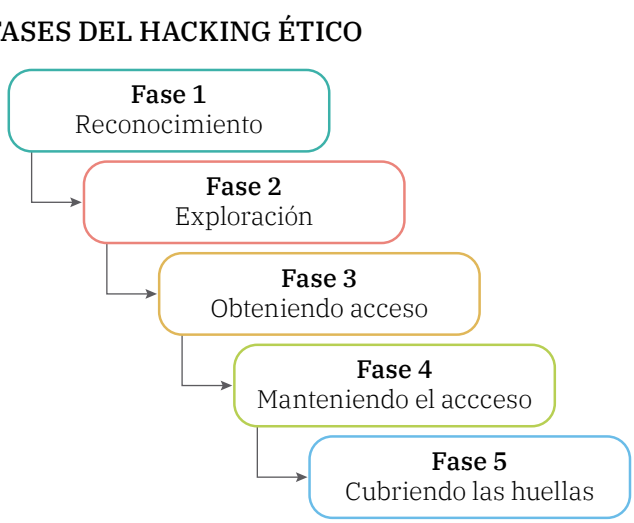


Tomado de: Silver & LLC, 2017

que estos a su vez realicen las mejoras pertinentes en la seguridad del sistema, eliminando los riesgos y amenazas que presentaba el sistema de dicha organización. Así pues, los hackers éticos son necesarios en todas las compañías, ya que dan parte de tranquilidad al constatar que la información está siendo tratadas de forma segura y responsable (Blum, Course Hero, 2007).

Dentro de la cultura del hacking ético estos expertos además de investigar y crear también comparten información de cómo evitar que la mayoría de los sistemas sean vulnerados por otros, los conocidos como hackers (Osorio, 2016). Se especula que el hacking comenzó alrededor de los años 70's cuando John Draper (conocido como el capitán Crunch) logró generar una señal con la que evitaba la tarificación de llamadas, y de esta manera, no solo hacía llamadas gratis, sino que también, junto con Denny Teresi, tomó el control de sistemas telefónicos centrales (Solís S. M., 2018). Por otro lado, se empezó a hablar de hacking ético a mediados de 1995 cuando el hacker Kevin David Mitnick, que era buscado por el FBI durante más de dos años, es atrapado con la ayuda de Tsutomu Shimomura, un experto en seguridad informática (M. J. E 2019). En la figura 2 se mencionan las diferentes fases que típicamente se utilizan en un proceso de hacking ético.

Figura 2. Fases del hacking ético



Tomado de: Roberto González, 2019

Inteligencia artificial y hacking ético

La Inteligencia artificial es una rama de la informática que se dedica al uso de algoritmos y creación de mecanismos que pueden mostrar comportamientos considerados inteligentes, es decir, que tengan, idealmente, capacidad de ra-

zonamiento y aprendizaje como el ser humano. Sus orígenes se remontan a 1956 cuando John McCarthy, un prominente informático que posteriormente recibió el Premio Turing en 1971, introduce el término al describir al tipo de máquina capaz de encontrar una solución luego de serle asignada una tarea desconocida. Actualmente, la IA se utiliza en diversos escenarios como lo son la educación, los mercados, la manufactura, el gobierno y el legislativo, la salud, etc. (Rouse, TechTarget, 2017) y (Chas, AURO PORTAL, 2020).

Cuando se examina el papel de la IA en la ciberseguridad desde el grado sistemático, existen tres áreas de gran impacto: robustez, resistencia y respuestas del sistema. En las tres variantes, el potencial de la IA se combina con graves riesgos éticos. Si no se afrontan, estos riesgos podrían arremeter contra la adopción de la IA en la ciberseguridad o generar problemas importantes en nuestras sociedades (Taddeo, 2019). La IA para pruebas de software es una nueva área de investigación y desarrollo y se hace con el fin de diseñar software que sea capaz de autoevaluar y auto curar. Lo que significa que puede ayudar a verificar y validar el software. Esto podría tener un efecto de ralentización frente a las vulnerabilidades encontradas. En relación con eso, como la validación y verificación la realizaría el sistema, se liberaría la carga laboral y tediosa generada en los humanos. Sin embargo, aunque la IA puede ayudar a hacer pruebas más rápidas y eficientes a un sistema dado, se debe tener cuidado al delegar tanta responsabilidad en las pruebas, pues esto podría conllevar una deslocalización de expertos. Los humanos son importantes porque son los expertos en ciberseguridad, ellos poseen un mejor concepto de ética, por ende, deben seguir realizando pruebas en los sistemas y además siempre es bueno un juicio de expertos (Taddeo, 2019).

Algoritmos en inteligencia artificial

Una creciente preocupación en las organizaciones actuales respecto a las implicaciones de la inteligencia artificial es el aprendizaje automático y profundo debido a que se teme que el riesgo de ataques sea mayor ya que los sistemas se optimizan y mejoran con mayor recurrencia y facilidad lo que puede implicar que se realicen ataques más rápidos y con mayores niveles de impacto. Sin embargo, la IA también puede identificar vulnerabilidades de los sistemas que a menudo puede ser imposibles de encontrar para los expertos humanos (Taddeo y Floridi, 2018). Dentro de estás técnicas de identificación de vulnerabilidades y protección de sistemas se encuentran algoritmos o tipos de aprendizaje definidos en inteligencia artificial que se distribuyen en tres grupos principales (MOYA, 2016):

Aprendizaje por refuerzo (RL, Reinforcement Learning):

El adquirir conocimientos por refuerzo radica en el número de ensayos recurrentes que realiza una máquina fundamentados en “pruebas y errores” usando el menor tiempo posible en encontrar la solución o el resultado esperado. Es posible entenderlo usando como ejemplo el juego de batalla naval, en el cual el objetivo es hundir los barcos del contrincante y para lo cual se aplican una serie de intentos en los que el sistema aprende a punta de pruebas y errores.

Aprendizaje supervisado (Supervised machine learning):

Se apoya en una serie de patrones predictivos que utilizan datos de adiestramiento, es decir que, en un grupo de datos ingresados al sistema, esta toma dichos datos, los analiza, los transforma y muestra una salida donde se encuentran los resultados esperados. Un ejemplo de este tipo de aprendizaje es el usado en vehículos autónomos.

Aprendizaje no supervisado (Unsupervised machine learning):

Este tipo de estudio es muy similar al anterior con la diferencia de que este se apoya únicamente en los datos de entrada. Es decir que el algoritmo utiliza un auto adiestramiento sin tener en cuenta ningún tipo de indicación externa. Como ejemplo está el agrupamiento de objetos no etiquetados, en un grupo de subconjuntos que son llamados Clústers.

Ventajas y desventajas del uso de IA

(Yucatan D. , 2018)

La inteligencia artificial, como tecnología emergente y en desarrollo, conlleva evidentes beneficios en su implementación, pero puede también implicar riesgos o desafíos importantes que deben tener en cuenta con el fin de mitigar o evitar su impacto nocivo. A continuación, se enlistan las principales ventajas y desventajas que podrían presentarse como consecuencia del uso de la inteligencia artificial.

Ventajas

- Automatiza los procesos: la inteligencia artificial ayuda a liberar carga laboral permitiendo que algunas máquinas ejecuten trabajos repetitivos automáticamente y sin supervisión alguna.
- Potencia las tareas creativas: gracias a la característica anterior el personal que se dedicada a ejecutar tareas repetitivas puede ejecutar otro tipo de labores, con seguridad de mayor interés para sus organizaciones.
- Aporta precisión: en las compañías de manufacturación la inteligencia artificial ha logrado que el proceso de producción sea más efectivo y preciso, ya que las máquinas son entrenadas para tomar decisiones sin supervisión humana.
- Reduce el error humano: las máquinas que aplican la inteligencia artificial son capaces de detectar anomalías en las piezas o productos que produzca la organización y que son indetectables por el personal del área de trabajo.
- Reduce los tiempos empleados en análisis de datos: hace posible que esta tarea se ejecute en el menor tiempo posible, aumente la producción y la efectividad sin descuidar la calidad.
- Mantenimiento predictivo: esto quiere decir que la AI ejecuta su propio mantenimiento en las máquinas de producción cuando no están operando y así controla el desgaste de piezas y ofrece un mejor rendimiento a la organización.
- Mejora en la toma de decisiones tanto a nivel de producción como de negocio: la inteligencia artificial puede pronosticar escenarios donde resuelve situaciones en muy corto tiempo y también prever problemas a largo plazo (Integra, Nexusintegra.io, 2020).

Desventajas

- La IA se ejecuta a través de programas desarrollados con lenguajes de programación como Python y MATLAB, y estos a su vez están sujetos a procesos de actualizaciones y mejoras, así como también el programa que se encarga de aplicar la AI, lo cual puede generar errores inesperados o problemas de compatibilidad.
- El uso de la IA en cualquier escenario representa una importante inversión de capital, recurso humano altamente capacitado y recursos tecnológicos en ocasiones difícil de adquirir.
- La IA puede contribuir a la reducción considerable de mano de obra.
- La cantidad de expertos en IA respecto a su demanda es aún muy baja.

Contexto actual de hacking ético

Contexto mundial

La era de la transformación digital es una realidad para la mayor parte de la industria y, consecuentemente, las amenazas informáticas para empresas y clientes son crecientes. Cada vez se pueden encontrar dispositivos nuevos que se conectan desde cualquier lugar y en cualquier momento. Podría decirse que a mayor evolución tecnológica existe un mayor número de amenazas, pero también un mayor número de tácticas y recursos para tratar de hacerles frente. En noticias son expuestos solamente ciertos delitos cometidos a grandes empresas, pero no hay mayor eco para las demás, cuyos ataques pueden ser incluso peores, ya que el objetivo de los ciberdelincuentes se amplía día a día y los datos personales, ya sean de redes sociales, historiales médicos o hasta archivos bancarios son motines sustanciales para los hackers. Este tipo de ataques varía dependiendo del tipo de daño por el

que se dirijan, a partir de lo cual se pueden tener los siguientes tipos de delincuentes:

- Cibernéticos, que buscan lucrarse por este medio realizando distintos tipos de fraudes.
- Hacktivistas, que se dedican a detectar las fallas en los sistemas informáticos, son motivados por la política o el entorno social, un ejemplo famoso dentro de esta clasificación es la organización Anonymous. (Rochina, 2016)
- Terroristas cibernéticos, que se basan en el entorno cibernético para llevar a cabo los atentados a sectores sensibles como el sector salud, sector defensa, sector bancario, etc. (Rodrigo, 2020)
- Ciberespías, que comprometen la ciberseguridad en las organizaciones al robar información valiosa de clientes y empleados, y que generalmente venden en el mercado negro.

Así pues, por la variedad en los tipos de ataques que puede sufrir una organización, el firewall ya no es suficiente y la búsqueda de alternativas se seguridad es un tema cada vez de mayor importancia. Aquí por esto que empieza a aumentar la demanda de expertos en seguridad de TI, pues las empresas ya se están renovando y ahora buscan hacer autoevaluaciones frecuentes para saber cómo se están protegiendo los datos y en general saber el estado en que se encuentran en cuanto a seguridad informática: saber si sus datos se encuentran con la debida protección, si son sensibles y desde qué dispositivos pueden ser accedidos. (Vela, 2019)

Contexto nacional

El hacking ético en Colombia aún no se reconoce a nivel profesional y tan solo pueden reconocer algunas pocas áreas laborales en las cuales es posible encontrar un hacker o hablar del tema. Algunos ejemplos son los profesionales que trabajan para empresas de seguridad informática o de desarrollo de aplicaciones, las personas que trabajan en el área de sistemas, ya sea en soporte o mantenimiento de computadores, o también en áreas comerciales, pues por su quehacer profesional se enteran brevemente del tema, y finalmente están los empíricos entusiasmados por los sistemas informáticos que aprovechan su tiempo libre para practicar y ganar experticia. Es evidente que el hacking ético no tiene ese reconocimiento que debería tener ya que hablando de personas que tienen estas habilidades o conocen del tema resulta ser bastante costoso, se puede decir que es un grupo al que muy pocos pueden acceder, así sea con la intención de dar sus conocimientos para ayudas de las empresas o problemas específicos, también hay que tener en cuenta que en la cultura hacker el mejor es aquel que cumple con sus objetivos sin ser detectado ni reconocido, y para que los espacios académicos apoyen esto sería muy difícil ya que la intención de todos los que lo practiquen no va a ser siempre con buenas intenciones (Federico Ivan Gacharna 2009 pág. 2).

Algo que entorpece el pensamiento colombiano es ese estigma que tiene el hacking ya que centran su atención en noticias de robos o informes que han ocurrido a lo largo de la historia, y de esta forma lo ven como gente delincuente aprovechando su conocimiento para sacar beneficios de los demás, las instituciones evitan tocar estos temas por temor que puedan ser ellas mismas las afectadas. Sin embargo, en Colombia hay una pequeña comunidad de hacker éticos que se clasifican en tres grupos principales. Para empezar, están aquellos afortunados que se encuentran ya sean en puestos del estado o instituciones del país sirven para fines del estado o se podría decir para el bien del país que este tipo de gente es el opuesto del hacker común ya que estos cuentan con un reconocimiento y un nivel de interacción diferente. Por otro lado, el grupo mayoritario lo conforman personas con educación superior (distinta a la ingeniería de sistemas) o aficionados sin estudios avanzados, que generalmente usan software desarrollado por terceros y cuentan con conocimientos empíricos insuficientes y se enfrentan a barreras importantes para acceder a información de calidad lo cual los limita para lograr resultados significativos. Finalmente, se identifican también aquellos que se apasionan con el tema y anhelan saber sobre hacking puesto que puede ser una opción de vida o sencillamente porque se trata de un tema de vanguardia, pero si bien su curiosidad sobre el tema es tan grande que buscan por diferentes medios aprender, están desinformados sobre lo que verdaderamente significa ser un hacker (Federico Iván Gacharna 2009 pág. 2).

Marco regulatorio del hacking ético

Escenario mundial

Uno de los desafíos fundamentales para la estabilidad de la ciberseguridad son los marcos normativos y regulatorios. En 2018 algunos senadores de EE. UU sugirieron a las organizaciones embestir a los ciberdelincuentes como respuesta a los ataques generados pero la propuesta no fue bien vista ya que esto puede no poner fin a los ataques sino por el contrario intensificarlos. Es por esto que la comunidad internacional necesita establecer una regulación que implemente un comportamiento ético en el ciberespacio y establezca una autoridad que tenga la capacidad de supervisar aspectos como:

- Acuerdos con normas internacionales.
- Verificar el cumplimiento de los estados con las normas tanto nacional como internacionalmente.
- Iniciar investigaciones a presuntos implicados con delitos informáticos.
- Exponer infracciones acerca de las normas y las fuentes de ilegalidad – atacar ciberataques.
- Imponer sanciones adecuadas.

Las normativas son necesarias para garantizar un comportamiento responsable, ético y con base en la protección de los derechos individuales. Un esfuerzo coordinado que incluya a la sociedad, la política, las organizaciones y la academia podrá contrarrestar y efectuar estrategias para que la IA sea imprescindible en fomentar la seguridad y la ética. En muchas ocasiones se ha debatido como abordar contramedidas y controles para limitar el uso malicioso de la IA en el ámbito de la ciberseguridad. Además, la regulación debe tener en cuenta el uso de los principios éticos y jurídicos a ciudadanos, empresas y estados. De acuerdo con lo anterior, la Comisión europea inició un estudio a mediados de 2018 con el propósito de establecer unas directrices éticas como base para el uso y el desarrollo legal de la IA (Taddeo 2019).

Se publicó en abril de 2019 el informe “Ethics Guidelines for Trustworthy Artificial Intelligence”. Las directrices que se recomiendan se basan en el uso de la IA confiable, lo que conlleva que esta debe atender a todas las leyes y regulaciones, debe respetar los principios y valores éticos y debe ser robusta teniendo en cuenta una perspectiva técnica y observando el entorno social. Los requisitos fundamentales consisten en propiciar sociedades equitativas apoyando la intervención humana, ser capaces de resolver errores o incoherencias durante todas las fases del ciclo de vida útil de los sistemas de IA, y asegurar la privacidad y el control de la información. Por otra parte, algunas normas que establecen la regulación de la seguridad de la información y que siempre deben ser tenidas en cuenta son:

- Norma ISO/IEC 27001: la Organización Internacional de Estandarización (ISO) creó la normativa ISO/IEC 27001 con el fin de establecer la seguridad de la información en las empresas.
- Norma ISO/IEC 27002: es el “Código de buena práctica para la gestión de la seguridad de la información”. Garantiza que la información, los equipos y las instalaciones de procesamiento de información de una organización, se encuentren protegidos contra el código malicioso (MinT (27015:2012, 2012).

Escenario nacional

Actualmente en Colombia no existen normas que prohíban el uso de inteligencia artificial en hacking ético. Sin embargo, en 2017 el Gobierno Nacional, la Cancillería, los Ministerios de Justicia, Defensa y las TIC presentaron al Congreso de la República un proyecto enmarcado en el convenio de Budapest. Este se aprobó tanto en la plenaria del senado como en la cámara de representantes y se divide en tres pilares esenciales. El primero menciona los delitos que se catalogan como se muestra en la figura 3 y que también se pueden clasificar como:

- Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos: por ejemplo, el acceso indebido a sistemas que contengan datos personales o confidenciales.
- Delitos informáticos: fraude tecnológico, modificación de información o datos no autenticados en algún sistema. (JIMÉNEZ, 2016)

- Delitos de contenido: divulgación de pornografía infantil, información en contra de la integridad sexual.
- Delitos relacionados con infracciones de derechos de autor: reproducción y emisión de contenido sin consentimiento del creador intelectual o titular de la patente.

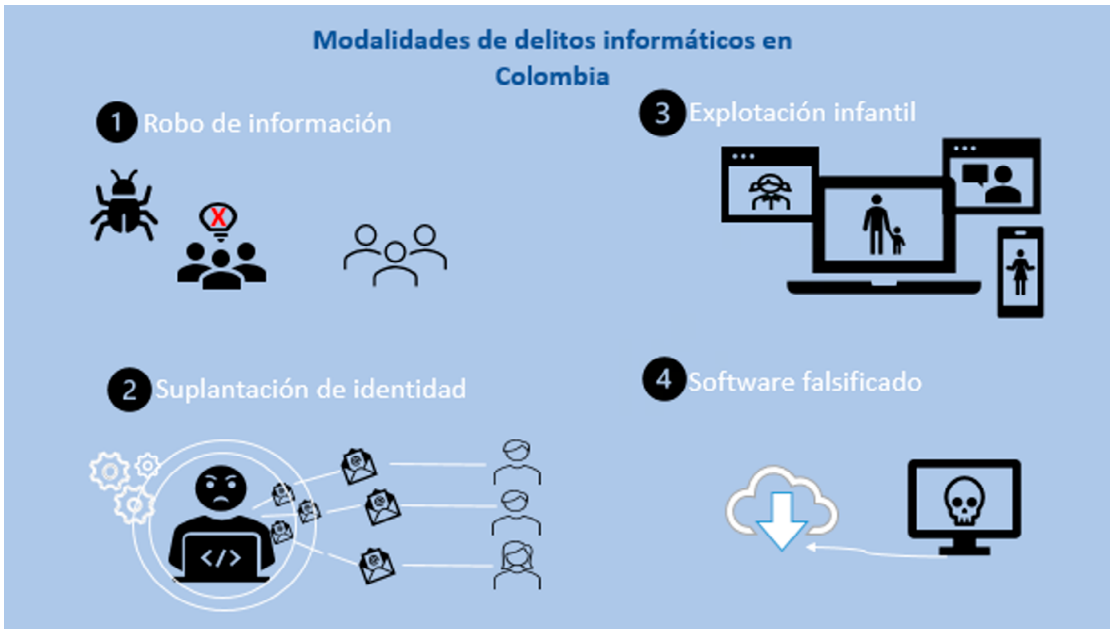
De acuerdo con lo anterior Colombia ha tenido que modificar sus marcos normativos como parte de las herramientas necesarias para hacer frente al cibercrimen y de paso promulgar el uso de la ética informática. Entre las leyes más conocidas, se enfatiza la ley 1273 de 2009, en donde se actualizó el código penal y se creó "la protección de la información y los datos". Asimismo, también está la ley 1581 de 2012, que tiene por objeto la protección de los datos personales registrados en cualquier base de datos o archivos y la recolección, modificación, uso y tratamiento por parte de entidades públicas o privadas. Por otra parte, está la Ley Estatutaria de Inteligencia y Contrainteligencia (1621 de 2013) que fortaleció el marco jurídico que permite a los organismos de inteligencia y contrainteligencia cumplir con su misión constitucional y legal (Lopez, 2019).

Vulnerabilidades de software detectadas con hacking ético

Para nadie es un secreto que en el software está expuesto a un sinfín de vulnerabilidades de seguridad y para poder hablar de las diferentes tecnologías que se han desarrollado para fortalecer dichas vulnerabilidades, es necesario conocer primero las amenazas. A continuación, se describen de manera sencilla los diferentes tipos de desarrollos de software creados para aprovechar estas vulnerabilidades y atacar el sistema, mejor conocidos como malware, y que además se muestran en la figura 4: (Bortoni, 2020)

- Bot: Software diseñado para ejecutarse de manera automática generalmente en línea, estos se envían a varios pc y estos esperan silenciosamente las instrucciones de los agresores.
- Adware: Software diseñado para bombardear los pc con anuncios publicitarios de manera automática.
- Spyware: Software diseñado para vigilar y escudriñar a la víctima. Se encarga de recopilar pulsaciones de las teclas, para capturar datos y conseguir contraseñas secretas.

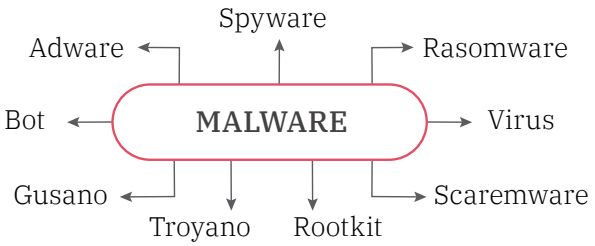
Figura 3. Modalidades de delitos informáticos en Colombia.



Tomado de: GFSI, 2018

- Rasomware: Software diseñado para mantener secuestrado un sistema o los datos de dicho sistema hasta que se efectué un pago por parte de la víctima.
- Scareware: Software diseñado para que el usuario ejecute una acción para evitar que el sistema operativo colapse y es allí donde el equipo queda infectado.
- Skimming: Consiste en el robo de información por medio de la clonación de tarjetas de crédito.
- Virus: Software diseñado para unirse a otros archivos ejecutables y así poder infectar automáticamente a varios equipos.
- Troyano: Virus diseñado ataca los permisos del usuario que lo ejecuta estos se unen a archivos de audio, imágenes y juegos.
- Gusanos: Virus que se encarga de hacer que el tráfico de la red se ponga muy lento.

Figura 4. Clasificación de diferentes tipos de malware.



Tomado de: Kheng, 2018

Por ejemplo, en el año 2015 el gusano de código rojo infecto a más 6586 servidores en tan solo 19 horas. “En 2015, una vulnerabilidad importante, llamada SYNful Knock, se descubrió en Cisco IOS. Esta vulnerabilidad permitió a los atacantes obtener el control de los routers de nivel empresarial.” (luz, 2015).

Existen otras vulnerabilidades que se pueden encontrar en bases de datos y otros sistemas. Sin embargo, es posible utilizar hardening para asegurar el sistema mientras se reduce el número de vulnerabilidades, que consiste en eliminar software, servicios y usuarios redundantes en el sistema, es decir, entradas para los ciberdelincuentes, y haciendo pruebas de intrusión a través de las herramientas tecnológicas. Una técnica muy utilizada últimamente por las aplicaciones y sistemas es el cifrado de datos, sirve para proteger información confidencial que es transmitida por satélite o por alguna red de comunicaciones. Los datos son codificados mediante algoritmos y no pueden ser descifrados por alguien externo excepto personas autorizadas que cuenten con claves para ser interpretados. En la mayoria de las pruebas se cuentan con herramientas Open Source licenciadas, esto es muy importante tanto para el ambito etico como el legal. A continuación, se mencionaran algunos ejemplos:

- SQLMAP: Esta herramienta permite detectar errores como inyección de SQL, realiza pruebas que delimitan el acceso a la información de las bases de datos, busca vulnerabilidades y soluciona problemas al mismo tiempo.
- NMAP: Muy utilizado en pruebas de penetración para administradores de sistema. Tiene la capacidad de verificar si existen aplicaciones con denegaciones en el servidor y se pueden realizar procesos de auditoria en la red.

Vulnerabilidades de hardware detectadas con hacking ético

Estas se presentan más que todo en defectos en diseño de ***hardware*** como la memoria RAM en estas existen pequeños dispositivos electrónicos que por su cercanía con otros dispositivos de sus mismas características son vulnerables, ya que la reescritura de memoria que se realiza constantemente en un PC es utilizada en un ataque llamado Rowhamer, este puede recuperar todos los datos de las celdas de memoria cercanas así estas estén blindadas. Otras vulnerabilidades que se pueden presentar se hacen evidente cuando se utilizan dispositivos USB, discos extraíbles y discos de estado sólido. Estas vulnerabilidades son más fáciles de controlar y de detectar que las de software, pero es necesario no bajar la guardia y aplicar el hacking ético a cabalidad. Por ejemplo, en el año 2010 se creó un virus que se insertó a través de una memoria USB en una planta de energía Atómica, este virus se propagó a través de 1000 máquinas y les ordenó autodestruirse eliminando toda información que estas poseían (BBC, 2015).

Recomendaciones

Dentro de las alternativas de mitigación de ataques cibernéticos más importantes se pueden incluir la capacitación de empleados y clientes acerca de cómo prevenir violaciones en el sistema, y de la importancia de realizar el cambio periódico de las contraseñas, ejecutar juiciosamente las actualizaciones sugeridas por el departamento de TI, validar la autenticación de sitios web, entre otros. También es necesario asegurarse de que todos los sistemas estén limpios y que no se hayan instalado puertas traseras y que no haya nada comprometido a través de auditorías trimestrales de todo el sistema, utilizar encriptación de archivos sobre todo los que se transfiere a través de la red, y vacunar todos los dispositivos electrónicos que son utilizados y controlar el acceso a estos.

Conclusiones

Es necesario mencionar que el hecho de ser hacker no implica ser un criminal con una máscara frente a un computador en algún rincón oscuro, y cambiar esa percepción que se ha ido construyendo en el imaginario colectivo a lo largo de la historia es una tarea compleja. Es preciso entender que de cada uno depende con qué fines va a utilizar su conocimiento adquirido, no importa la fuente, y que contar con mucho conocimiento no implica necesariamente atender el marco legal y regulatorio que aplique.

Y es aquí es donde el hacker ético juega un papel muy importante para la seguridad, al ser un experto en el área de computación y redes que, con el consentimiento de una persona u organización y atendiendo a normas legalmente establecidas, realiza ataques periódicos a los sistemas con el fin de encontrar vulnerabilidades que un cibercriminal o un hacker malicioso puede aprovechar para cometer sus delitos. Se encargará de verificar el software y redes a través del pentesting, donde puede determinar las vulnerabilidades de un sistema para luego reportar a las organizaciones los fallos detectados,

También es necesario tener en cuenta que todo lo que tenga presencia en internet y todo lo que capture datos o información, estará expuesto a vulnerabilidades y que la mayor parte de la responsabilidad en ciberseguridad dependerá del usuario ejecutor del intercambio de información, más aún, teniendo en cuenta que a medida que pasa el tiempo los ataques evolucionan constantemente porque los sistemas deben ser evaluados y actualizados continuamente, y para detener ataques y mantener la confianza depositada ya sea por los clientes o por la organización, la ciberseguridad debe ser robusta y permanente.

Bibliografía

27015:2012, I. T. (2012, 12). ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection. 18. Retrieved from http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=43755

Aceros, J. C. (2004). El error como acontecimiento y el hacking como aprovechamiento creativo del mismo. *Scripta Nova Revista electrónica de geografía y ciencias sociales.*

Álvarez, M. M. (2019). La ciberseguridad en Colombia. *Seguritecnia,* 50-51.

Andes, U. d. (2019). Inteligencia artificial. *Contacto*, 6.

Asobancaria. (2018, 08 06). Retos de Colombia en ciberseguridad a propósito de la adhesión al "Convenio de Budapest". *Semana Económica 2018* (1148), 1,2,5,6. Retrieved 06 20, 2020

Avila, M. A. (2019, 02 07). *Hacking ético: impacto en la sociedad.* Retrieved from http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/4919/00005096.pdf?sequence=1&isAllowed=y

Banafa, A. (2018, Marzo 27). *bbvaopenmind.com/.* Retrieved Octubre 20, 2020, from https://www.bbvaopenmind.com/tecnologia/inteligencia-artificial/inteligencia-artificial-en-ciberseguridad-retos/

BBC. (2015, 10 11). *BBC.COM.* Retrieved from https://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet

Blum, R. (2007, Marzo 25). *Course Hero.* Retrieved Junio 04, 2020, from Course Hero: https://www.coursehero.com/file/29043414/BT-INS-IT-Industry-Survey-Ethical-Hackingpdf/

Blum, R. (2007, 03 27). ETHICAL HACKING.

Bortoni, C. O. (2020, Junio 22). *TyN Magazine.* Retrieved from Uso de Hacking Ético para Reforzar las Vulnerabilidades: https://www.tynmagazine.com/uso-de-hacking-etico-para-reforzar-las-vulnerabilidades/

Calle, M. J. (2017, Agosto 07). *ittrendsinstitute.org.* Retrieved 10 20, 2020, from http://www.ittrendsinstitute.org/perspectives/item/ia-y-ciberseguridad

Capgemini. (2019, Noviembre 05). *digitalbizmagazine.com/.* Retrieved 10 20, 2020, from https://www.digitalbizmagazine.com/inteligencia-artificial-y-ciberseguridad/

Chas, A. (2019). *AURA PORTAL.*

Chas, A. (2020, Mayo 15). *AURA PORTAL.* Retrieved Junio 08, 2020, from AURO PORTAL: https://www.auraportal.com/es/que-es-la-inteligencia-artificial/

Dialani, P. (2020, 10 15). *hackercar.com.* Retrieved 10 20, 2020, from https://hackercar.com/ia-ciberataques/

Estretegicos, I. E. (2019). *Documentos de Seguridad y Defensa 79, La inteligencia artificial aplicada a la defensa.* España: Ministerio de Defensa. Retrieved 10 2020, 23, from La Inteligencia artificial aplicada a la defensa: Dialnet-LaInteligenciaArtificialAplicadaALaDefensa-731297.pdf

Floridi, L. y. (2016). ¿Qué es la ética de los datos? *Transacciones filosóficas de la Royal Society A: Ciencias Matemáticas, Físicas e Ingeniería* (374(2083)). Retrieved 06 06, 2020, from https: //doi.org/10.1098/ rsta.2016.0360

Gonzalez, P. (2015). Pentesting persistente y estratégico: nuevos ataques y nuevos modelos. *Red seguridad,* 66-68.

González, R. C. (2019). *eHack.* Retrieved 06 29, 2020, from Las fases del Hacking Ético: https://ehack.info/las-fases-del-hacking-etico/

Grupo Funcional de Seguridad Informática, U. (2018, 07 27). *Nueva modalidad de delitos informáticos en Colombia.* Retrieved 06 29, 2020, from Nueva modalidad de delitos informáticos en Colombia: https://noticias.unad.edu.co/index.php/gidt/2333-nueva-modalidad-de-delitos-informaticos-en-colombia

Integra, N. (2020, 01 17). *NEXUSINTEGRA*. Retrieved from https://nexusintegra.io/es/blog/ventajas-y-desventajas-de-la-inteligencia-artificial/

Integra, N. (2020, Enero 17). *Nexusintegra.io.* Retrieved Junio 10, 2020, from Nexusintegra.io: https://nexusintegra.io/es/blog/ventajas-y-desventajas-de-la-inteligencia-artificial/

JIMÉNEZ, C. Á. (2016, Octubre 05). *La historia detrás de cinco 'hackers' colombianos y sus delitos.* Retrieved from https://www.eltiempo.com/archivo/documento/CMS-16719460

Jiménez, F. J. (2015). Ciberseguridad e inteligencia. *Red seguridad: revista especializada en seguridad informática, protección de datos y comunicaciones,* 70-72.

Lopez, L. (2019, Junio 06). *Blue radio.* Retrieved from El colombiano reconocido como uno de los mejores hackers del mundo: https://www.bluradio.com/tecnologia/el-colombiano-reconocido-como-uno-de-los-mejores-hackers-del-mundo

Luis Aemando Gaona Paez, J. E. (2019). *Ciberseguridad y Ethical Hacking.* Retrieved from https://acofipapers.org/index.php/eiei/article/view/248/244

luz, S. d. (2015, 09 17). *REDES ZONE.* Retrieved from https://www.redeszone.net/2015/09/17/descubren-varios-routers-cisco-infectados-por-synful-knock-un-malware-oculto/

M., J. E. (2019, 10 16). *IMPACTO TIC.* Retrieved from https://impactotic.co/hacking-etico-y-ciberdelincuentes/

Mansueti, M. (2018). Parano1a Digital. In M. Mansueti, *Parano1a DIGITAL* (p. 304). eBook. Retrieved from https://www.megustaleer.com.co/libros/paranoia-digital/MAR-015268

MinTic. (2019, 10). *Ministerio de Tecnologías de la Información y las Comunicaciones.* Retrieved from Estándares de la Industria: https://www.mintic.gov.co/arquitecturati/630/propertyvalues-8158_descargable_2.pdf

Miranda, A. L. (2015). Guía de ataques, vulnerabilidades, técnicas y. *ReCIBE. Revistas Electrónica de Computación, Informática, Biomedicina y Electrónica,* 6-10.

MOYA, R. (2016, Marzo 25). *Jarroba.* Retrieved Junio 10, 2020, from Jarroba: https://jarroba.com/que-es-el-clustering/

Moya, R. (2016, 03 25). *Jarroba.com.*

Muñoz, J. R. (2017). CiberÉtica como ética aplicada: una introducción. *Dilemata,* 52-61.

Orozco, F. J. (2016, 11 12). Prezi.com. Retrieved from https://prezi.com/yg8sd8sbe-jm/historia-de-hacking/

Osorio, F. V. (2016, Noviembre 12). *Prezi.* Retrieved Junio 09, 2020, from Prezi: https://prezi.com/yg8sd8sbe-jm/historia-de-hacking/

P., R. S. (2019, 07 20). *SEGURIDAD DIGITAL EL MERCURIO.* Retrieved Junio 08, 2020, from https://seguridaddigital.emol.com/noticias/hacking-etico/la-inteligencia-artificial-y-la-automatizacion-del-hacker/

Parraga, A. C. (2017). *ANÁLISIS DE LOS DELITOS INFORMÁTICOS EN EL ACTUAL SISTEMA.* Retrieved 06 20, 2020, from https://repository.unilibre.edu.co/bitstream/handle/10901/11041/AN%C3%81LISIS%20DE%20LOS%20DELITOS%20INFORM%C3%81TICOS%20EN%20EL%20ACTUAL%20SISTEMA%20PENAL%20COLOMBIANO%20revisado%20NHJ%20OK.pdf?sequence=3&isAllowed=y

Prieto, J. V. (2019, Noviembre 12). *Ia-latam.com.* Retrieved 10 20, 2020, from https://ia-latam.com/2019/11/12/el-reto-de-una-robotica-e-inteligencia-artificial-honesta-con-las-personas/

Raymond, E. S. (2000). Breve historia de la cultura hacker. *biblioweb,* 3-7.

Rochina, P. (2016, 05 18). *Hacktivismo: Qué hay detrás de este movimiento activista?* Retrieved from https://revistadigital.inesem.es/informatica-y-tics/hacktivismo/

Rodrigo, B. (2020, Enero 19). *El comercio.* Retrieved from Terrorismo Informatico: https://www.elcomercio.com/opinion/columnista-opinion-elcomercio-terrorismo-informatico.html

Rouse, M. (2017, Abril 27). *TechTarget.* Retrieved Junio 10, 2020, from TechTarget: https://searchdatacenter.techtarget.com/es/definicion/Inteligencia-artificial-o-AI

Rouse, M. (2017, 04). *TechTarget 20.*

Rubio, Y. (2019). Los claroscuros de la ciberseguridad. *Revista Tribuna Norteamericana,* 18-21.

Sif, I. (2019, Enero 10). Deloitte.com, 10. Retrieved 10 20, 2020, from https://www2.deloitte.com/content/dam/Deloitte/co/Documents/technology/Tendencias_tecnologicas_2019%20(Reporte%20Completo).pdf

Solís, S. M. (2018, Abril 24). *ICEMD.* Retrieved Junio 09, 2020, from ICEMD: https://www.icemd.com/digital-knowledge/articulos/que-es-hacking-etico-en-que-marco-legal-se-mueve/

Solís, S. M. (2018, 04 24). *ICEMD ESIC.* Retrieved from https://www.icemd.com/digital-knowledge/articulos/que-es-hacking-etico-en-que-marco-legal-se-mueve/

Soriano, A. G. (2012). HACKING ÉTICO: MITOS Y REALIDADES. *Revista seguridad unam*.

Summa, R. (2020, Enero 14). *revistasumma.com.* Retrieved 10 20, 2020, from https://revistasumma.com/hacking-etico-por-que-es-necesario/

Taddeo, M. (2014b). La lucha entre libertades y autoridades en la era de la información. *Ciencia y Etíca de la Ingenieria.* Retrieved 06 14, 2020, from https://doi.org/10.1007/s11948-014-9586-0

Taddeo, M. (2017a). Los límites de la teoría de la disuasión en el ciberespacio. *Filosofía y Tecnología.* Retrieved 6 6, 2020, from https://doi.org/10.1007/s13347-017-0290-2

Taddeo, M. y. (2018b). Cómo la IA puede ser una fuerza para el bien. *Ciencia* (361(6404)), 751-752. Retrieved 06 14, 2020, from Ciencia: https://doi.org/10.1126/science.aat5991

Tapia, Á. G. (2011). Inteligencia artificial. *Manual formativo de ACTA.*

Tegmark, M. (2018). *Vida 3.0.* In M. Tegmark, Vida 3.0 (p. 496). Tauros.

Vela, E. C. (2019, Octubre 28). *Canalceo.* Retrieved from En el punto de mira de los ciberespías: https://canalceo.com/en-el-punto-de-mira-de-los-ciberespias/

Yucatan. (2018, 05 19). *Yucatan.com.mx.* Retrieved from https://www.yucatan.com.mx/tecnologia/ventajas-desventajas-la-inteligencia-artificial

Yucatan, D. (2018, Mayo 19). *yucatan.com.mx.* Retrieved Junio 10, 2020, from yucatan.com.mx: https://www.yucatan.com.mx/tecnologia/ventajas-desventajas-la-inteligencia-artificial