# DETERMINACIÓN DE LOS ATAQUES CIBERNÉTICOS CLAVES A TRAVÉS DE LA TÉCNICA MICMAC Y SU INFLUENCIA ECONÓMICA FINANCIERA AL ADQUIRIR HERRAMIENTAS DE SEGURIDAD AUTOMATIZADA

# DETERMINATION OF KEY CYBER ATTACKS THROUGH THE MICMAC TECHNIQUE AND THEIR ECONOMIC AND FINANCIAL INFLUENCE WHEN ACQUIRING AUTOMATED SECURITY TOOLS

Maira Bastidas Gómez[1]
Heybertt Moreno Díaz[2]
Paulo Sexto Oyola Quitero[3]

**Resumen**

El objetivo de la presente investigación fue determinar las técnicas de ataques cibernéticos claves más comunes a tener en cuenta al momento de desarrollar estrategias de ciberseguridad y herramientas adecuadas que se puedan aplicar a cualquier empresa, su activo o amenaza, su relación económica financiera y evidenciando la relación de influencia y dependencia de estos ataques. El estudio se tipificó como cualitativo, se realizó revisión documental y se aplicaron las técnicas lluvia de ideas y MICMAC. Como resultados se obtuvo que ataques como Botnets, Machine learning poisoning, Exploitation of vulnerabilities entre otros, son ataques que requieren un seguimiento y monitoreo riguroso que permita verificar la efectividad del control de ataques comunes en general, debido a que dependen del comportamiento de los ataques clave. Se concluye que el ataque social engineering, es determinante, a la hora de formular estrategias y herramientas que repelen ciberataques. Se recomienda formular estrategias y herramientas enfocadas a los ataques clave y a los determinantes.

**Palabras clave:** Ciberseguridad, datos personales, influencia económica, privacidad, códigos maliciosos

**Abstract**

The purpose of this research was to determine the most common key cyber-attack techniques to consider when developing cybersecurity strategies and appropriate tools that can be applied to any company, asset or threat, its financial economic relationship and evidencing the relationship of influence and dependence of these attacks. The study was classified as qualitative, documentary review was carried out and brainstorming and MICMAC techniques were applied. As a result, it was obtained that attacks such as Botnets, Machine learning poisoning, Exploitation of

Fecha de recepción: Septiembre de 2019 / Fecha de aceptación en forma revisada: Diciembre 2019

[1]Estudiante de Ingeniería de sistemas de la Universidad de Cartagena, integrante de grupo de investigación – INGESINFO. ORCID: https://orcid.org/0000-0003-0657-135X. Email: maira2121@gmail.com

[2]Especialista en Telecomunicaciones. Docente Investigador del Programa de Ingeniería de Sistemas, Universidad de Cartagena ORCID: https://orcid.org/0000-0003-3228-8371. Email: hmorenod@unicartagena.edu.co

[3]Magister en Educación, Universidad de Cartagena. Docente Investigador del Programa de Administración de Empresas, Universidad de Cartagena. ORCID: https://orcid.org/0000-0002-6811-8246. Email: poyolaq@unicartagena.edu.co

vulnerabilities among others, are attacks that require a rigorous monitoring and monitoring that allows to verify the effectiveness of the control of common attacks in general, because they depend on the behavior of the attacks key. It is concluded that social engineering attack is decisive, when formulating strategies and tools that repel cyber-attacks. It is recommended to formulate strategies and tools focused on key attacks and determinants.

**Keywords:** Cybersecurity, personal data, economic influence, privacy, malicious codes

## Introducción

Los sistemas de información se enfrentan a atacantes sofisticados que combinan múltiples vulnerabilidades para penetrar en las redes (Singhal y Ou, 2017). La seguridad general de una red no se puede determinar simplemente contando el número de vulnerabilidades, sino que se debe comprender cómo se pueden combinar y explotar para organizar un ataque. A lo largo de la historia, se han registrado grandes ataques que van desde el robo de decenas o cientos de millones de registros, credenciales de inicio de sesión, información financiera o datos personales (Ding et al., 2018).

Entre los ataques más famosos se encuentran, la divulgación de datos de Yahoo en 2013, en el cual, las cuentas de cada cliente fueron violadas en ese periodo; la información personal comprometida sobre historial crediticio de Equifax en 2017; el acceso no autorizado durante cinco años, al sistema de reservas del hotel Marriott, en el cual se obtuvo acceso a nombre, número de pasaporte e información de tarjetas de crédito de sus clientes; el acceso a la información privada del tesoro de documentos digitales de First American Financial Corp en 2019, los cuales contenían, números de Seguridad Social y cuentas bancarias, y los datos de usuarios de la red social Facebook expuesta públicamente en los servidores de computación en la nube de Amazon (Valinsky, 2019).

Lo anterior evidencian que nadie está exento de sufrir violaciones a su privacidad, razón por la cual, la seguridad de redes y sistemas de información constituye una de las preocupaciones en el marco nacional e internacional (Carrillo, 2018). Por lo anterior, para garantizar una mayor seguridad en las redes y sistemas de información, la unión europea ha tomado medidas, como la publicación de la directiva NIS, la cual busca mejorar la seguridad de las redes y sistemas de información. De igual manera, con los protocolos de seguridad se definen los mecanismos que permitan la protección de la información, buscando que exista siempre confidencialidad, disponibilidad e integración de la información (Peláez, 2002).

En este sentido, los sistemas de seguridad cibernética se diseñan de dos maneras: (1) se identifican las amenazas y se compran e implementan herramientas de seguridad cibernética ("COTS") disponibles con la expectativa de mitigar las amenazas identificadas; o (2) se compra y despliega una selección de los mejores COTS actuales con la expectativa de hacer el mejor trabajo posible en la protección de las empresas, no obstante, una limitante de estas herramientas es que tienen visibilidad y se especializan solo en los tipos de dominios, eventos y amenazas que se supervisan e informan (Mead et al., 2017), es decir, que solo se detectan e informan sobre los vectores de ataque dentro de cada compañía específica o tipo de activo o amenaza, esto limita su efectividad por cual podría representar una mala inversión. Por lo anterior, la finalidad del presente estudio, es determinar las técnicas de ataques claves más comunes para tener en cuenta al momento de desarrollar estrategias y adquirir herramientas adecuadas que se puedan aplicar a cualquier empresa, activo o amenaza, evidenciando la relación de influencia y dependencia de estos ataques.

## Metodología

La presente investigación se tipificó como cualitativa debido a que se busca principalmente la expansión de los datos e información obtenida (Hernández, Fernández y Baptista ,2014). En este caso, sobre los ataques a trasvés de la determinación de los más utilizados. Para lograrlo se utilizó la revisión documental y la técnica lluvia de ideas, de la cual se aplicó a varios profesionales en seguridad en redes. Como resultados de la aplicación de estas dos técnicas, se obtuvieron los quince (15) ataques más comunes. Como técnica de análisis de datos se utilizó el método MICMAC, la cual permite identificar los factores o variables claves a través de una matriz de n x n, la cual se representa en un plano que clasifica las variables según su ubicación en: claves, autónomas, determinantes y de resultados. Esta técnica, proporciona un análisis donde se distinguen los problemas presentes en el sistema y se analizan sus comportamientos (Arango y Cuevas, 2014). En este estudio, se busca determinar los ataques clave, autónomos determinantes y de resultados y, por consiguiente, la influencia y la dependencia entre sí.

## Resultados y discusión

Al aplicar la metodología antes expuesta, como resultado de la revisión documental y la lluvia de ideas, se obtuvieron 15 ataques, los cuales se presumen son los más comunes, para una mejor descripción, en el Cuadro 1 se muestran los detalles.

| N° | Nombre corto | Nombre largo | Descripción |
|---|---|---|---|
| **1** | AIF | Artificial intelligence fuzzing | Con esta técnica, se introducen datos no válidos, inesperados o semi-aleatorios en interfaces para dar seguimiento a fallas, aserciones de códigos fallidos, fugas de memoria, entre otros, para aprovechar el aprendizaje automático y desarrollar programas de fuzzing automatizados, que aceleran el proceso de identificación de vulnerabilidades en un entorno controlado. |
| **2** | AMC | Attacks by Malignant Codes (Malware) | Los códigos malignos o malware son un tipo de software que tiene como objetivo infiltrarse o dañar un sistema de información o recurso específico sin el consentimiento de su propietario, para obtener algún beneficio. |
| **3** | AUA | Attacks by User Authentication (Gross Force) | Realizar todas las confinaciones posibles para obtener un usuario y/o contraseña. |
| **4** | BTS | Botnets | Una botnet es una red de equipos infectados por códigos maliciosos, se les conoce como equipos "zombies" porque son equipos controlados remotamente por cibercriminales. El objetivo de este ataque, es enviar órdenes a los equipos zombies haciendo uso de sus recursos, pasando desapercibido por los usuario. |

| | | | |
|---|---|---|---|
| **5** | CIN | Code injection | En esta técnica se intenta inyectar código que es interpretado/ejecutado por la aplicación, como resultado de fallas de seguridad habituales por la falta de validación apropiada de entradas y salidas de datos. |
| **6** | DOS | Denial of service | Denegación de servicio o DoS, impedir que el usuario acceda a su información o servicios. |
| **7** | EOF | Evasion of firewall and IDS | Técnicas utilizadas para saltar controles basados en firewall e ids. |
| **8** | EOV | Exploitation of vulnerabilities | Aprovechamiento de fallas de seguridad en software para obtener acceso al sistema de la víctima, escalar privilegios, etc o por lo menos causar un DoS. |
| **9** | INS | Social engineering | Con este ataque se obtiene mediante engaños información sensible de la víctima. |
| **10** | MLP | Machine learning poisoning | Envenenamiento del motor de aprendizaje automático utilizado para detectar malware, dejándolo ineficaz, debido a que el modelo de aprendizaje automático aprende de los datos de entrada. Si ese grupo de datos está envenenado, la salida también se envenena. |
| **11** | PES | Privilege escalation | Una vez el atacante entra en la máquina de la víctima escalara privilegio (mediante explotación de vulnerabilidades) para obtener la cuenta de más privilegios del sistema (root, system). |
| **12** | PHG | Phising | Engaño realizado a la víctima (generalmente vía email) |
| **13** | REG | Reverse engineering | Modificar el lenguaje ensamblador de un ejecutable. |
| **14** | SCM | Scam | Esta técnica consiste en la estafa a través de medios electrónicos. El objetivo es lucrar directamente de los datos de los usuarios, los cuales obtienen a través del engaño. La estrategia más común, son los anuncios de haber ganado un premio extraordinario o realizar peticiones de ayuda caritativa. |
| **15** | SHG | Session hijacking | Secuestro de sesiones, mayormente tcp. |

*Cuadro 1. Ataques más comunes*

La columna 1 corresponde al número de la variable, la segunda al nombre corto, el cual fue asignado para una mejor manipulación al aplicar el método MICMAC. La tercera columna corresponde al nombre largo de la variable y, por último, la columna de la descripción. En este caso, la variable N° 1, es el ataque con nombre corto: AIF, nombre largo: Artificial intelligence

fuzzing, y su descripción: Con esta técnica, se introducen datos no válidos, inesperados o semi-aleatorios en interfaces para dar seguimiento a fallas, aserciones de códigos fallidos, fugas de memoria, entre otros, para aprovechar el aprendizaje automático y desarrollar programas de fuzzing automatizados, que aceleran el proceso de identificación de vulnerabilidades en un entorno controlado.

Seguido, el ataque con nombre corto: AMC, nombre largo: Attacks by Malignant Codes (Malware) y su descripción: Los códigos malignos o malware son un tipo de software que tiene como objetivo infiltrarse o dañar un sistema de información o recurso específico sin el consentimiento de su propietario, para obtener algún beneficio. Y así, se describen los quince ataques encontrados como más comunes.

Una vez terminada la tabulación de los datos, se procedió al análisis, con la técnica MICMAC, el siguiente paso, fue diligenciar la matriz de relaciones de influencia directa, la cual se observa en la Figura 1. La matriz se llena con valores de cero (0) a tres (4), donde cero (0) significa que la relación es nula, uno (1) relación débil, dos (2) relación moderada, tres (3) relación fuerte y cuatro (4) significa que la relación es potencial, no obstante, la representación de la relación potencial, se representa con la letra P.

*Figura 1. Matriz de influencia directa (MID)*

Matriz de influencia directa (MID) | Plano de influencia directa | Grafo directo | Otros datos

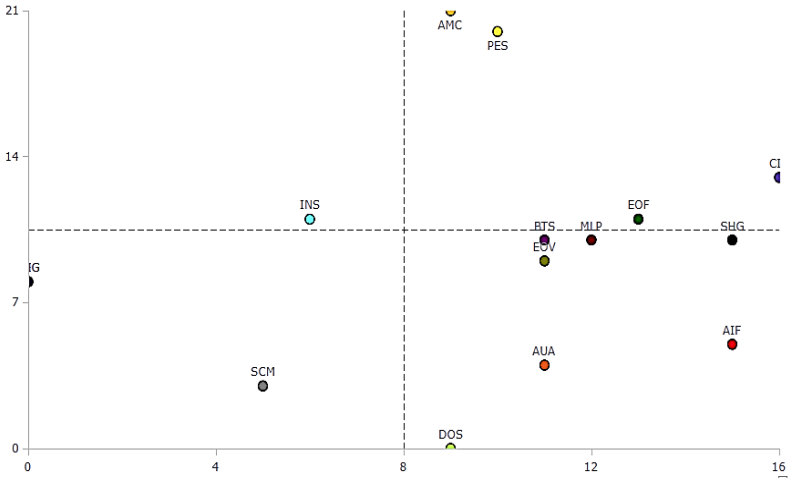
| | AIF | AMC | AUA | BTS | CIN | DOS | EOF | EOV | INS | MLP | PES | PHG | REG | SCM | SHG | I.D. |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| AIF | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 2 | 0 | 0 | 0 | 0 | P | 0 | 1 | 5 |
| AMC | 2 | 0 | 0 | 1 | 3 | 3 | 2 | 3 | 0 | 2 | 1 | 0 | 0 | 3 | 1 | 21 |
| AUA | 0 | 0 | 0 | 0 | 0 | 2 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 4 |
| BTS | 0 | 1 | 1 | 0 | 2 | 2 | 0 | 0 | 0 | 0 | 2 | 0 | 0 | 0 | 2 | 10 |
| CIN | 2 | P | 3 | 1 | 0 | 1 | 0 | 0 | 0 | 2 | 3 | 0 | 0 | 0 | 1 | 13 |
| DOS | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| EOF | 0 | 3 | 0 | 0 | 3 | 0 | 0 | 1 | 0 | 0 | 3 | 0 | 0 | 0 | 1 | 11 |
| EOV | 3 | P | P | 2 | P | 0 | 0 | 0 | 0 | 3 | P | 0 | 0 | 1 | 0 | 9 |
| INS | 0 | 2 | 3 | 2 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | P | 0 | P | 2 | 11 |
| MLP | 0 | 1 | 0 | 0 | 1 | 0 | 3 | 3 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 10 |
| PES | 3 | P | 3 | 2 | 3 | 0 | 3 | 0 | 0 | 3 | 0 | 0 | P | 0 | 3 | 20 |
| PHG | 0 | 0 | P | 2 | 0 | 0 | 0 | 0 | 3 | 0 | 0 | 0 | 0 | P | 3 | 8 |
| REG | 3 | 0 | 0 | 0 | 3 | 0 | 2 | P | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 8 |
| SCM | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 3 | 0 | 0 | 0 | P | 0 | 0 | 3 |
| SHG | 2 | 2 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 2 | 0 | 0 | 0 | 1 | 0 | 10 |
| D.D. | 15 | 9 | 11 | 11 | 16 | 9 | 13 | 11 | 6 | 12 | 10 | 0 | 0 | 5 | 15 | 143 |

En la Figura 1 se observa que la variable AIF (Artificial intelligence fuzzing) tiene relación débil (1) con la variable SHG (Session Hijacking), una relación moderada (2), con las variables EOF (Evasion of firewall and IDS) y EOV (Exploitation of vulnerabilities), una relación potencial (P) con la variable REG (Reverse engineering) y la relación con el resto de las variables, es nula (0).

Con respecto a la variable N° 2, AMC (Attacks by Malignant Codes (Malware)), esta mantiene una relación débil (1) con las variables BTS (Botnets), PES (Privilege escalation) y SHG (Session Hijacking); una relación moderada (2) con las variables AIF (Artificial intelligence fuzzing), EOF (Evasion of firewall and IDS) y MLP (Machine learning poisoning); mantiene una relación fuerte (3) con las variables CIN (Code injection), DOS (Denial of service), EOV (Exploitation of vulnerabilities) y SCM (Scam); mantiene una relación nula (0) con el resto de variables, no se registraron relaciones potenciales (P). de esta manera se puede interpretar los resultados de la matriz de influencia directa.

Una vez llena la matriz de influencia directa, se representa en un plano de cuatro cuadrantes, en el cual se clasifica según la ubicación, en variables clave (cuadrante I, superior derecho), determinantes (cuadrante II, superior izquierdo), autónomas (cuadrante III, inferior izquierdo) y de resultados (cuadrante IV, inferior derecho). A continuación, en la Figura 2, se observan los resultados obtenidos.

*Figura 2. Plano de influencia Directa*




En el cuadrante de las variables clave, se ubicaron las variables: AMC, PES, CIN y EOF, que corresponden a los ataques Attacks by Malignant Codes (Malware), Privilege escalation, Code injection y Evasion of firewall and IDS, respectivamente. Lo cual significa que son muy influyentes y muy dependientes, por tanto, perturban el funcionamiento normal del sistema (Martelo et al., 2017). Son por naturaleza inestables y se corresponden con los retos del sistema. En resumen, son los ataques que se deben tener en cuenta a la hora de formular las estrategias de ciberseguridad, debido a que representan retos que propician cambios en el sistema a un nivel más óptimo. A continuación, en el Cuadro 2, se muestran los ataques clave y las vulnerabilidades que estos ataques aprovechan. Cabe resaltar, que etas vulnerabilidades se encuentran en el Top ten de OWASP (2017), el cual se basa en el envío de datos de empresas especializadas en seguridad de aplicaciones y una encuesta de la industria que fue realizada por más de 500 personas.

| Ataques Clave | Vulnerabilidades OWASP (2017) |
|---|---|
| Attacks by Malignant Codes (Malware) | Code injection, Exhibition of sensitive data, XML External Entities (XXE), Cross-Site Scripting XSS, Insecure Deserialization, Injection. |
| Privilege escalation | Security Misconfiguration, |
| Code injection | Cross-Site Scripting XSS, Exhibition of sensitive data, XML External Entities (XXE), Injection, |
| Evasion of firewall and IDS | Broken Authentication, Broken Access Control. |

*Cuadro 2. Ataques clave y vulnerabilidades involucradas*

En cuanto al ataque con malware, las herramientas para generarlos se han extendido rápidamente en Internet, facilitando que personas sin experiencia puedan crearlos (Kang y Won, 2018), por lo anterior es difícil controlar esta situación y es lo que convierte a esta variable en clave, a la hora de formular estrategias de ciberseguridad. Por otro lado, debido a la falta de comprensión del conocimiento de control de acceso por parte de los desarrolladores, se producen

errores lógicos en el proceso de desarrollo del programa, lo que conduce a la existencia de vulnerabilidades de control de acceso entre estos, Privilege escalation (Ma, Yan y Xie, 2019).

El ataque Code injection por su parte, es una de las técnicas más famosas que amenazan las aplicaciones web, debido a que compromete la confidencialidad, integridad y disponibilidad del sistema de una aplicación en línea (Nofal y Amer, 2019). Este ataque puede causar serios problemas de seguridad, como: omisión de autenticación, fuga de privacidad y ejecución de código arbitrario. Es una variable clave, porque es difícil de controlar, debido a la diversidad de ataques y a la dificultad del descubrimiento. En cuanto al ataque Evasion of firewall and IDS, los atacantes pueden enviar paquetes de ataques evasivos que intentarán evitar ser detectados por el IDS, y se pueden obtener herramientas para automatizar tales ataques (Tanabe et al., 2018), lo cual lo convierte en una variable inestable y, por lo tanto, clave.

En el cuadrante de las variables determinantes, solo se ubicó la variable INS, que corresponde al ataque social engineering. Lo cual significa según su evolución, que será el freno o motor del sistema. En este ataque, la puerta de entrada es el usuario, y en el campo de la ciberseguridad, el factor humano es el elemento más crítico y si el usuario cede ante este ataque, el sistema se verá frenado. Al respecto, los expertos en seguridad conocen la importancia de los comportamientos de seguridad de las personas, como, por ejemplo, la gestión de contraseñas, la prevención de ataques de phishing y similares. Sin embargo, según Corradini y Nardelli (2019), las organizaciones aún carecen de una cultura de ciberseguridad para gestionar los riesgos de seguridad relacionados en particular con el factor humano. Por lo cual se sugiere dar más valor a esta variable y educar a los usuarios, para que esta variable sea propulsora y determine el comportamiento adecuado del sistema.

En el cuadrante de las variables autónomas aparecen tres variables: PHG, REG y SCM, que corresponde a los ataques: Phising, Reverse engineering y Scam, respectivamente, en el caso de los ataques Phising y Reverse engineering, obtuvieron las mismas coordenadas, esto significan que tiene la misma relevancia. Estos ataques son poco influyentes o y poco dependientes, constituye parte poco determinante para el futuro del sistema y no constituye un reto, sin embargo, es necesario dar más valor a estas variables, debido a que, según su evolución, pueden cambiar de estado.

Para el caso del cuadrante de las variables de resultado, se ubicaron siete variables: BTS, MLP, EOV, AUA, AIF, DOS y SHG, que corresponden a los ataques: Botnets, Machine learning poisoning, Exploitation of vulnerabilities, Attacks by User Authentication (Gross Force), Artificial intelligence fuzzing, Denial of service y Session hijacking, respectivamente. Estas variables, poseen baja influencia y alta dependencia, y unidas a las variables clave, suelen ser indicadores descriptivos de la evolución del sistema. son variables que se deben abordar o tratar a través de las que dependen en el sistema.

Una botnet es una colección de agentes de software distribuidos en dispositivos en red bajo el control de un servidor de origen. Se usan con frecuencia para alojar aplicaciones de servidor, que son controladas por un servidor de origen y, por lo tanto, pueden usar flujo rápido para evitar la detección (Yen et al., 2014). En el ataque Machine learning poisoning por su parte, los atacantes inyectan una pequeña cantidad de puntos corruptos en el proceso de entrenamiento. Tales ataques de envenenamiento se han demostrado prácticamente en la generación de firmas de gusanos, filtros de spam, detección de ataques DoS, clasificación de malware PDF, reconocimiento de dígitos escritos a mano y análisis de opinión (Jagielski et al., 2018). Lo anterior evidencia que las variables de resultado, dependen del comportamiento de las variables clave, determinantes y autónomas, debido a estas actúan en forma negativa si se permiten los ataques ubicados en los otros cuadrantes.

En resumen, se requiere un seguimiento y monitoreo riguroso que permita verificar la efectividad del control de ataques comunes en general.

Lo descrito, representa una base sólida para el desarrollo de estrategias de ciberseguridad y la obtención de herramientas idóneas para hacer frente a los ataques. En este sentido, se obtienen beneficios financieros debido a que se puede realizar una inversión adecuada en aquellas herramientas que cumplan con las características requeridas. Esto guarda similitud con el estudio de (Bucur & Babulak, 2019) donde se plantea que el crecimiento continuo de las amenazas de ciberseguridad y la falta de efectividad de diferentes opciones de ciberseguridad como los sistemas de control de acceso y cortafuegos, se convertido en un incentivo para aprender sobre diversas metodologías de ciberataques con el fin de hacer frente a los ciberatacantes, de esta forma se pueden conocer las especificaciones necesarias con las cuales debe contar las herramientas de ciberseguridad a implementar por lo cual se puede efectuar una inversión idónea.

## Conclusiones

Debido a que los ataques cibernéticos son cada vez más sofisticados, es necesario que las organizaciones estén preparadas para enfrentar de manera adecuada el desafío que representa la ciberseguridad. En este estudio se clasificaron los 15 ataques cibernéticos más comunes en: claves, determinantes, autónomos y de resultados. Los resultados evidencian que los ataques clave presentan una alta dependencia y una alta influencia respecto a los determinantes, autónomos y de resultados, esto significa que son los ataques que se deben tratar con prioridad, debido a que presentan características comunes con los demás ataques y los cambios que se realicen a favor o en contra de estos, se verán reflejados en el sistema. Teniendo en cuenta lo anterior, desde el punto financiero, y se evitan inversiones innecesarias en herramientas poco efectivas, debido a que la clasificación de técnicas de ataques claves más comunes permite determinar las características con las cuales debe contar la herramienta de ciberseguridad y realizar una inversión adecuada.

## Referencias bibliográficas

Arango, X. A., & Cuevas Pérez, V. A. (2014). Método de análisis estructural: matriz de impactos cruzados multiplicación aplicada a una clasificación (MICMAC) (Doctoral dissertation, Tirant Lo Blanch).

Bucur, C., & Babulak, E. (2019). Security validation testing environment in the cloud. IEEE International Conference on Big Data, (págs. 4240-4247). Los Angeles. doi:10.1109/BigData47090.2019.9006202.

Carrillo, M. R. (2018). Seguridad de redes y sistemas de información en la Unión Europea: ¿un enfoque integral? Revista de Derecho Comunitario Europeo, 22(60), 563-600.

Corradini, I., & Nardelli, E. (2019). Social Engineering and the Value of Data: The Need of Specific Awareness Programs. In International Conference on Applied Human Factors and Ergonomics (pp. 59-65). Springer, Cham.

Ding, D., Han, Q. L., Xiang, Y., Ge, X., & Zhang, X. M. (2018). A survey on security control and attack detection for industrial cyber-physical systems. Neurocomputing, 275, 1674-1683.

Fernández, A. V., & Rodríguez, J. M. C. (2017). Análisis de las ciberamenazas. Cuadernos de estrategia, (185), 97-138.

González C. Rafael E., Pérez, Jaime M., Tarón D. Arnulfo. (2016). Desarrollo y validación de un modelo matemático para describir el crecimiento de lactobacillus acidophilus microencapsulado en un sistema binario compuesto por goma gelana. Revista @limentech,Ciencia y Tecnología Alimentaría. ISSN: 1692-7125. Volumen 14 N°1. Pp. 74 -83.

Hernández, R., Fernández, C. y Baptista, M. (2014). *Metodología de la investigación*, México: McGraw Hill.

Hernández Bieliukas, Y. C., & Aranguren Peraza, G. (2016). Patrón tecnopedagógico: ruta de aprendizaje basado en actividades comprensivas. *Revista vínculos*, *13*(2), 149-158. https://doi.org/10.14483/2322939X.11671

Jagielski, M., Oprea, A., Biggio, B., Liu, C., Nita-Rotaru, C., & Li, B. (2018, May). Manipulating machine learning: Poisoning attacks and countermeasures for regression learning. In 2018 IEEE Symposium on Security and Privacy (SP) (pp. 19-35). IEEE.

Kang, J., & Won, Y. (2018). Malware Classification Using Machine Learning. In Advances in Computer Science and Ubiquitous Computing (pp. 279-284). Springer, Singapore.

Ma, L., Yan, Y., & Xie, H. (2019). A New Approach for Detecting Access Control Vulnerabilities. In 2019 7th International Conference on Information, Communication and Networks (ICICN) (pp. 109-113). IEEE.

Martelo. R., JIMENEZ-PITRE, I., & VILLABONA-GÓMEZ (2017). Determinación de factores para deserción de estudiantes en pregrado a través de las técnicas lluvia de ideas y MICMAC. Revista Espacios. Vol. 38 (Nº 20) Año 2017.

Mead, J., Vasatka, J. E., & Craig, J. A. (2017). U.S. Cybersecurity system with differentiated capacity to deal with complex cyber-attacks. Patent Application No. 14/872,698.

Nofal, D. E., & Amer, A. A. (2019). SQL Injection Attacks Detection and Prevention Based on Neuro-Fuzzy Technique. In International Conference on Advanced Intelligent Systems and Informatics (pp. 722-738). Springer, Cham.

OWASP (2017). Top 10 Web Application Security Risks. Recuperate of: https://owasp.org/www-project-top-ten/.

Singhal, A., & Ou, X. (2017). Security risk analysis of enterprise networks using probabilistic attack graphs. In Network Security Metrics (pp. 53-73). Springer, Cham.

Tanabe, R., Ueno, W., Ishii, K., Yoshioka, K., Matsumoto, T., Kasama, T., ... & Rossow, C. (2018). Evasive malware via identifier implanting. In International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment (pp. 162-184). Springer, Cham.

Pardo Garcia A, Castellanos González L. (2017). Automatización de Ambientes en Invernaderos Simulando Escenarios Futuros, Revista Colombiana de Tecnologías de Avanzada, ISSN: 1692-7257. Volumen1–Número 29-2017.

Palma Cardoso, E., Alarcón Linares, A. F., & Hernández Pava, E. A. (2018). Diseño de un sistema informático (software) para automatizar los procesos contables en el sector mecánico automotriz del régimen simplificado. *Revista Innova ITFIP*, *2*(1), 62-70. Recuperado a partir de http://revistainnovaitfip.com/index.php/innovajournal/article/view/29

Peláez R. S. (2002) Análisis de seguridad de la familia de protocolos TCP/IP y sus servicios asociados, Edición I, junio de 2002. Recuperado de http://es.tldp.org/Manuales-LuCAS/doc-Seguridad-tcpip/Seguridad_en_TCP-IP_Ed1.pdf.

Valinsky, J. (2019). 7 de los mayores hackeos de la historia. CNN en español. Recuperado de: https://cnnespanol.cnn.com/2019/08/01/7-de-los-mayores-hackeos-de-la-historia/.

Vergel, M. y Martínez, J. (2015). Filosofía gerencial seis sigma en la gestión universitaria. FACE, 15 (2). Recuperado de http://revistas.unipamplona.edu.co/ojs_viceinves/index.php/FACE/article/view/1619

Yen, C. T., Lugani, S., Mukhopadhyay, S., & Daftary, K. (2014). U.S. Patent No. 8,661,544. Washington, DC: U.S. Patent and Trademark Office.