ESCUELA SUPERIOR DE GUERRA

MAESTRÍA EN CIBERSEGURIDAD Y CIBERDEFENSA

MONOGRAFÍA

# ÁRBOLES DE ATAQUE EN LA EVALUACIÓN ECONÓMICA DE LAS INVERSIONES EN CIBERSEGURIDAD

BOGOTA, AGOSTO 29 DE 2022

ESCUELA SUPERIOR DE GUERRA

MAESTRIA EN CIBERSEGURIDAD Y CIBERDEFENSA

MONOGRAFÍA

# ÁRBOLES DE ATAQUE EN LA EVALUACIÓN ECONÓMICA DE LAS INVERSIONES EN CIBERSEGURIDAD

CARLOS ENRIQUE ROSERO CERÓN

TUTOR:

JAIDER OSPINA. MSC, ING.

BOGOTA, COLOMBIA, AGOSTO 2022

ÁRBOLES DE ATAQUE EN LA EVALUACIÓN ECONÓMICA DE LAS INVERSIONES EN CIBERSEGURIDAD

ROSERO CERÓN CARLOS ENRIQUE

FIRMA:
C.C 6.386.024
TEL: 315 8504337
CORREO ELECTRONICO: carlos@newsatint.com

TUTOR: JAIDER OSPINA. MSC, ING.

FIRMA:

PAGINA DE EVALUACION

CALIFICACIÓN EN NUMERO:

CALIFICACIÓN EN LETRAS: _____

OBSERVACIONES: _____

_____

_____

EVALUADOR:

FIRMA:

FECHA DE EVALUACION:

Agradezco a Dios por todas las bendiciones recibidas y colocarme en el sitio adecuado en el momento adecuado.
A mi amada esposa Maricel por su entendimiento, paciencia y apoyo para que pudiera terminar esta maestría.
A mi tutor MSC, Ing. Jaider Ospina por su acompañamiento, ánimo y guía,
A Terry Ingoldsby, por sus generosidad y guía con la herramienta Árboles de Ataque - SecurItree
A mis compañeros de la maestría, sin el apoyo de ellos, no lo hubiera logrado.
.

## Resumen

Dado que los ciberataques suponen una gran amenaza para las organizaciones, es necesario adoptar medidas de seguridad para proteger las redes y la información. La defensa contra estos ataques requiere importantes recursos e inversiones por parte de las organizaciones. Para los gerentes no les importa si se requiere un IPS/ IDS, un WAF, o un SIEM; lo que ellos necesitan evaluar es la relación costo/beneficio de dicha decisión. El nivel de riesgo residual después de implementar una contramedida debería ser criterio fundamental que oriente las inversiones de ciberseguridad. El no contar con una metodología sencilla para calcular el riesgo mitigado y su impacto en la expectativa de pérdida anual (ALE) que cada contramedida introduce en el eco sistema de ciberseguridad, lleva a los gerentes de IT a especular sobre la relación costo/beneficio de las inversiones. El modelo propuesto en este trabajo de grado usa los Árboles de Ataque para diagramar de forma sencilla y visual cómo se podrían llevar a cabo los diferentes escenarios de un ciberataque. Además, registra la interacción que se da entre el defensor y atacante, a través de variables de comportamiento que determinan la probabilidad de un ataque y el riesgo percibido. Esto permite estimar el riesgo mitigado después de implementar una contramedida. Con base en es esta información se priorizan las inversiones calculando el retorno de inversión de cada una de ellas (ROSI). La metodología propuesta, permite también estimar la predisposición que tienen las diferentes organizaciones a invertir en ciberseguridad, dependiendo del perfil de riesgo (tolerancia al riesgo).



Palabras Clave: Riesgo, ALE, Costo/beneficio, Ciberseguridad, Árboles de Ataque, ROSI, Tolerancia al Riesgo.

**Abstract**

As cyber-attacks threaten organizations, it is necessary to adopt security measures to protect networks and information. Defending against these attacks demands significant resources and investments from organizations. For managers, it is irrelevant whether an IPS/ IDS, a WAF, or a SIEM is required; what they need to evaluate is the cost/benefit ratio of such a decision. The level of residual risk after implementing a countermeasure should be a fundamental criterion guiding cybersecurity investments. Not having a simple methodology to calculate the mitigated risk and its impact on the annual loss expectation (ALE) that each countermeasure introduces in the cybersecurity eco-system, leads IT managers to speculate on the cost/benefit ratio of the investments. The model proposed in this project uses Attack Trees to diagram, in a simple and visual way, how the different scenarios of a cyber-attack could be carried out. In addition, it registers the interaction between the defender and the attacker, through behavioral variables that determine the probability of an attack and risk perceived. This allows estimating the mitigated risk after implementing a countermeasure. Based on this information, investments are prioritized by calculating the return of investment for each one of them (ROSI). The proposed methodology also allows to estimate the predisposition of the different organizations to invest in cybersecurity, depending on the risk profile (risk tolerance).

Keywords: Risk, ALE, Cost/benefit, Cybersecurity, Attack Trees, ROSI, Risk Tolerance.

## TABLA DE CONTENIDO

## TABLA DE FIGURAS

## TABLA DE TABLAS

# INTRODUCCIÓN

## Formulación del problema.

La seguridad digital se está convirtiendo cada vez más en un tema importante dentro de la agenda de los líderes de las organizaciones, debido a la creciente dependencia de Internet en un mundo postpandemia COVID 19, cada vez nuestra superficie de exposición al riesgo de un ataque cibernético es mayor.

Los ciberataques realizados en una organización influyen en su rendimiento y economía. Los aspectos económicos que podrían verse afectados por la materialización de un ataque, incluyen márgenes de ganancia, capitalización de mercado e imagen de marca de la organización. Por tal razón, los gerentes se ven constante más presionados para realizar nuevas inversiones en ciberseguridad, para lo cual necesitan contar con criterios de priorización de la implementación de dichas contramedidas, ya que el presupuesto es reducido y las necesidades son muchas. Los sistemas de ciberseguridad lo conforman una triada de tecnología – procesos – personas. Los seres humanos siguen siendo el eslabón más frágil de la ciberseguridad.

Un ataque de un adversario suele estar dirigido al sistema de información de la organización. Una brecha ocurre cuando el ataque penetra y compromete el sistema de información, bien sea en su confidencialidad, en su integridad o en su disponibilidad. La recuperación ocurre cuando la pérdida es limitada y la organización puede volver a la primera etapa de defensa contra ataques. Las organizaciones recurren al uso de dispositivos tecnológicos en múltiples niveles de seguridad para reducir la frecuencia y gravedad de una brecha de seguridad, Behara et al. 2007.

Ciber-Seguridad consiste en el desarrollo de un ecosistema de protección para reducir los riesgos de las amenazas que existen en el ciberespacio. esto involucra la revisión dentro de la organización de los procesos, personas y tecnologías. Incluye perspectivas de seguridad preventiva, de detección y correctiva. La defensa eficaz depende de la selección de estrategias adecuadas de gestión de la seguridad entre las diferentes opciones disponibles, cada una con diferentes costos y beneficios potenciales.

El problema al cual se enfrenta el director de IT o el CISO de una compañía con recursos presupuestales limitados para invertir en la implementación de controles ciberseguridad, es como priorizar dichas inversiones, conforme a un análisis costo/ beneficio de cada una de ellas.

El riesgo cibernético calcula la posibilidad de que una amenaza se materialice causando la interrupción de las operaciones, así como una pérdida monetaria, o una pérdida de imagen o credibilidad, afectando los resultados de una organización debido a un impacto adverso en el valor de la marca y la capitalización de mercado (Mukhopadhyay et al, 2013). Las organizaciones deben decidir cuántos recursos deben invertir en ciberseguridad para minimizar las pérdidas debidas a los ciberataques (Roumani et al, 2015). La cantidad invertida en ciberseguridad es una decisión estratégica. Esta decisión debe basarse en un análisis de costo-beneficio para garantizar que los riesgos se aborden de manera adecuada (Mukhopadhyay et al, 2013).

Las redes sofisticadas de delincuentes, los sistemas altamente conectados en la red y el creciente valor de la información almacenada en internet permite que el acceso a la información sea distribuido globalmente a un número incontable de personas. Esto hace que las organizaciones sean más vulnerables a los ataques cibernéticos. Los cibercriminales tienen por objeto robar o suplantar identidades, el espionaje y/o la interrupción de las operaciones de infraestructura crítica.

Los ciberataques más comunes son la denegación de servicios, el malware, el virus, los gusanos o troyanos, los ataques basados en web y el phishing (Niño, 2015). Según KASPERSKY (2020) Es interesante observar que la cantidad de ataques DDoS (por sus siglas en inglés Distribut, Denial of Service), a recursos web educativos y administrativos se ha triplicado en comparación con el mismo período en 2019. Además, tales ataques en el primer trimestre de 2020 representaron el 19% del número total de incidentes, mientras que hace un año solo representaban el 11%.

El aumento del interés de los ciber-delincuentes en dichos recursos puede estar asociado con la propagación de la infección por COVID 19, lo que ha hecho que los servicios de educación a distancia y las reuniones virtuales, acceso remoto a servicios prestados por diferentes entidades sean más populares. Desde principios de 2020, la epidemia ha afectado a todos los sectores, ya que la mayoría de las actividades productivas, educativas y de entretenimiento se han traslado al ciberespacio. Es lógico suponer que también afecta al mercado de ataques DDoS. Además, en el futuro cercano, este efecto puede profundizarse aún más, ya que el virus del COVID acelero los procesos de transformación digital de la mayoría de las entidades públicas y privadas.

A la gerencia ejecutiva realmente no le importa que el sistema de detección de intrusiones (IDS) o el firewall protejan los servidores de la organización. En cambio, están más preocupados por conocer el impacto de tales medidas de seguridad en los resultados financieros finales. Es importante tener en cuenta que las inversiones en seguridad no se pueden traducir directamente en beneficios monetarios, pero pueden evitar pérdidas comerciales considerablemente. Por lo tanto, para describir la importancia de la inversión en seguridad, es esencial demostrar el impacto de la falta de mecanismo de seguridad sobre la productividad, o sobre la imagen de marca, o sobre las ventas, etc. Es decir, es muy importante identificar las variables económicas que se verían afectadas en caso de que se materialice un ataque, así como la percepción de dolor de lo que dicho

ataque significa. Por ejemplo, para el caso de un ataque de Denegación de servicios a una universidad, la percepción de dolor de estar fuera de servicio, es diferente que, para una tienda virtual, en el día sin IVA. Es decir, la tolerancia al riesgo de cada entidad es diferente. Por esa razón dos organizaciones (empresas) reaccionan diferente gerencialmente ante la misma amenaza cibernética. Es importante que los gerentes de seguridad expliquen la gravedad de la brecha de seguridad con respecto a una pérdida potencial para la organización. ROSI (Retorno de la inversión en Seguridad) es un enfoque eficaz para justificar tales inversiones, ya que ayuda a priorizar cual es la solución rentable, cual es la cantidad correcta de dinero para invertir en las diferentes contramedidas de seguridad.

Las formas tradicionales de enfrentar el análisis económico de las inversiones en ciberseguridad, generalmente se han hecho desde la perspectiva del defensor, no se tiene en cuenta el atacante dentro de ese análisis, y es muy importante modelar las variables de motivación y capacidades del atacante, para poder diseñar una solución acorde al perfil del atacante; no es lo mismo prepararse para una hacker amateur, que para una organización criminal con recursos técnicos y económicos mucho más grandes .

Una vez conocido la forma como los delincuentes cibernéticos se planea y ejecutan este tipo de ataques se puede diseñar un sistema defensa con las protecciones adecuadas, que eleve el costo y el tiempo necesario que requiere el atacante para lograr su objetivo criminal. Ya que debemos tener claro que impedir un ataque al 100% es prácticamente imposible. Debemos estar seguro que, si una organización criminal te definió como objetivo de ataque, todo será cuestión de dinero y tiempo para poder conseguirlo.

La defensa contra los ataques cibernéticos, requiere que las organizaciones realicen inversiones para poder protegerse de esos potenciales ataques a los que están expuestos. La tolerancia al riesgo

percibido esta correlacionado con el nivel de inversión en defensa cibernética. El problema para determinar la inversión optima que te proteja en el ciberespacio, se vuelve más complejo cuando se involucra en el análisis de variables asociadas al apetito y tolerancia al riesgo.

Existes trabajo de investigación previos documentados para realizar el análisis económico de inversiones en seguridad tales como Angulo (2020), Bistarelli (2006) y Yacobb (2019), pero ninguno de ellos incluye variables de comportamiento tales como apetito de riesgo y/o tolerancia al riesgo de la víctima.

El presente trabajo de investigación pretende desarrollar una metodología de evaluación económica de las inversiones en ciberseguridad que le permita a la alta dirección tomar decisiones que busquen disminuir el riesgo cibernético, optimizando el costo / beneficio de las contramedidas, involucrando dentro del análisis variables de comportamiento del atacante y de la víctima.

En un extremo encontraremos sistemas de protección redundantes de ciberseguridad con presupuestos inviables y en otro extremo sistema totalmente vulnerable, con un presupuesto de inversión desperdiciados. El objetivo es poder definir una metodología que permita evaluar la rentabilidad financiera de una inversión en ciberseguridad, que disminuya el riesgo, elevando el costo y el tiempo de implementación de un ataque cibernético, es decir, una metodología basada en el análisis de la amenaza, colocándonos en los zapatos del atacante. Existen una variedad de metodologías para ayudar a la gerencia de una compañía para tomar decisiones que buscan disminuir el riesgo residual de una amenaza, por ejemplo: NIST 8216; la mayorías de las cuales están basadas desde el punto de vista del defensor, donde el riesgo se estima basados en simples listas de chequeo de puntos de control de naturaleza general (ISO, 27001, 27032, NIST SP 800-53), pero dichas metodologías no tienen en cuenta el comportamiento del atacante y la tolerancia

al riesgo del defensor, cuyo dolor percibido por un ataque cambia entre las diferentes organizaciones.

Este trabajo pretende desarrollar una metodología de evaluación económica de inversiones de ciberseguridad basado en modelamiento de amenazas. La metodología debe permitir el análisis económico de las diferentes alternativas de inversión realizadas en ciberseguridad. Este trabajo complementar las metodologías derivadas de la revisión de los puntos de control definidos en las normas ISO o normas NIST, y la evaluación del riesgo de la norma ISO 31000, partiendo del conocimiento que tenemos de la taxonomía de las amenazas. La época en la cual podamos dormir tranquilos con la implementación de sistemas de gestión de ciberseguridad basados en las normas ISO y la inclusión de contramedidas simples con equipos de seguridad perimetral con lista de bloqueos y filtros simples, son cosas del pasado.

Con el pasar de la historia se han descubierto múltiples ciber amenazas que han provocado diferentes tipos de daños y perjuicios tanto a empresas en todos los sectores de la economía, como a gobiernos e instituciones, además, de los millones de usuarios que tienen o han tenido acceso a las tecnologías de la información. Estas amenazas desde los orígenes de la informática han ido evolucionando y creciendo a medida que las tecnologías de la información y la era del Internet han evolucionado, tanto en número como en tipo y variedad. Seguramente en este momento se está planeando o materializando un incidente cibernético en cualquier lugar del mundo, sin importar el sector económico o institución.

Según Yohai (2019) último informe sobre las *"Tendencias del Ciber-crimen en Colombia 2019"*, realizado por la CCITT y Policía nacional de Colombia, los ataques cibernéticos en las universidades en Colombia reflejan un crecimiento gradual pues la Policía Nacional en el año 2019 registro 10.000 casos, del total de los casos registrados 5.000 fueron denunciados como

infracciones a la Ley 1273 de 2009. En comparación al año 2018 las denuncias informáticas aumentaron en el 2019 un 10%. Los ataques más reportados por los estudiantes y directivos de los centros educativos es el phishing con un 50%, la suplantación de identidad un 20%, el envío de malware un 17% y los fraudes de pago en línea un13%. La motivación principal de los cibercriminales es obtener la mayor información posible para tener una ventaja económica sobre las víctimas. Los delitos informáticos más denunciados por las universidades en Colombia son: el hurto, los cibercriminales conocen que el dinero está en las cuentas bancarias por esta razón buscan comprometer los sistemas de la institución educativa para interactuar con la entidad bancaria, el segundo lugar, está la violación de datos personales, para obtener esta información los cibercriminales suplanta la personalidad de la víctima, el tercer delito es el acceso abusivo a sistema informático, en el cuarto lugar se encuentra la transferencia no consentida de activos y el quinto delito es el uso de software malicioso. Las universidades que más sufre ataques cibernéticos son las que están ubicadas en Bogotá, Honda Tolima, Cartagena, Antioquia y Amazonas

Los colegios y universidades mantienen grandes depósitos de datos sensibles, incluyendo información financiera y estadística de investigación costosa, por lo son objetivos principales para los hackers de todo el mundo. Además, las universidades son a menudo incapaces de defender adecuadamente contra los intentos de hacking debido a las limitaciones presupuestales y la falta de personal.

Como resultado de ello, las universidades son cada vez más vulnerables a los hackers informáticos, los cuales con anterioridad pudieron haberse centrado en grandes corporaciones.

En el sector educativo colombiano ha habido noticias de ataques cibernéticos a universidades: Según Donoso (2018), la Universidad de los Andes en el año 2015 en Bogotá, donde un estudiante utilizando un software registrador de teclas (key loggers), capturó la

contraseña de docentes para acceder al sistema de notas y poder alterarlas, suceden frecuentemente. Recientemente se registró la noticia en medios de amplia circulación, tal como lo referencia Serrano (junio 2021.) en la FM, que la Universidad del Bosque sufrió un ataque cibernético por parte de hackers el día 28 de junio de 2021 en horas de la madrugada. Estos delincuentes cibernéticos se apoderaron de todas las cuentas de correo electrónico de la universidad e incluso de la cuenta de la universidad alojada en la red social Twitter según informes dados por ese medio

Otros casos de Ciberataques los podemos ver referenciados en el artículo "The Lucrative Rewards of Hacking Higher Education" del portal UpGuard.com donde se mencionan los siguientes ataques a universidades de renombre en los Estados Unidos:

Universidad de Yale, agosto de 2011: 43.000 nombres y números de seguridad social de personal, estudiantes y exalumnos, son robados por los piratas informáticos a través de un servidor FTP sin protección.

Universidad de Stanford, julio de 2013: El sistema SUNet de Stanford se ve comprometida, dando a los hackers el acceso a todas las cuentas de usuario y contraseñas.

Universidad de Berkeley, diciembre 2014: 1.600 registros de los empleados y exempleados son robados de los servidores universitarios. Los datos comprometidos incluyen números de la Seguridad Social y de tarjetas de crédito.

Universidad de Harvard, mayo de 2015: La página web del Instituto de Política es hackeada por el grupo AnonGhost Pro-Palestina.

La carencia o deficiencia de una Política de Seguridad Informática, así como controles de seguridad deficientes o inexistentes sobre los sistemas críticos de información en Colegios y

Universidades, son un atractivo cada vez mayor para los atacantes informáticos. Como lo indica Megan (2016) en su artículo Colleges and universities are prime cyber attack targets.

De acuerdo con el reporte Internet Security Threat Report, 4 de abril del 2019 de la compañía Symantec, en el año 2018 el sector educativo se encontraba en el tercer puesto en reportar mayor número de brechas de seguridad a nivel de subsectores y en noveno lugar de acuerdo con el número de entidades expuestas a estas brechas.

El presente trabajo de investigación pretende en su primera fase hacer un análisis de las diferentes metodologías que existen para modelar las amenazas cibernéticas.

Posteriormente, entraremos a estudiar los principales ataques documentados a universidades.

Con base en la investigación realizada en las fases previas se definirá una metodología para analizar económicamente las inversiones en ciberseguridad basada en árbol de ataque, donde se incluye variables de comportamiento del atacante y de tolerancia al dolor de la víctima (Apetito de riesgo).

Finalmente, es importante tener en cuenta que el modelamiento de los ataques hace parte importante de las gestiones de riesgos. La gestión de riesgos implica principalmente dos factores: análisis del impacto del ataque y otro el análisis de la viabilidad de un ataque. El objetivo de esta tesis está orientado a valorar económicamente las diferentes alternativas de inversiones (controles en ciberseguridad) para de esta forma poder priorizar dichas inversiones dentro de un presupuesto restringido con el que cuenta una universidad.

## Pregunta de investigación.

En virtud de lo anterior se plantea la siguiente pregunta de investigación

¿Cómo definir los controles de ciberseguridad para una institución educativa superior que permita disminuir el riesgo cibernético optimizando la relación costo/beneficio, basado en el modelamiento de amenazas?

**Objetivo general**

Definir una Metodología para la evaluación costo/beneficio de puntos de control en ciberseguridad, para instituciones de educación superior, basada en Árboles de ataque, incluyendo variables de comportamiento del atacante y de la víctima (tolerancia al riesgo).

**Objetivos específicos**

1.Determinar la metodología o modelado de amenazas que permita incluir las variables de comportamiento del atacante y de la víctima (tolerancia al riesgo)

2.Hacer una investigación bibliográfica de los ataques cibernéticos documentados contra universidades a nivel global y en Colombia en forma específica.

3. Definir una metodología de evaluación económica de inversiones ciberseguridad para universidades en Colombia, basada en Árboles de Ataques, donde se refleje el comportamiento del atacante y de la víctima.

# 1. CAPITULO I

## **1.1.** Modelado de Amenazas

Antes de comenzar a exponer diferentes perspectivas de lo que es un modelado de amenazas es importante entrar a definir un marco teórico asociados a la metodología, caracterización y modelado de amenazas.

### **1.1.1.** Marco Teórico del Análisis de amenazas.

AMENAZA: Según NIST SP 800-30, Una amenaza es cualquier circunstancia o evento con el potencial de afectar negativamente las operaciones y los activos de la organización, de los individuos, o de la Nación, de un sistema de información, bien sea afectando la confidencialidad (a través del acceso no autorizado), la integridad (destrucción, divulgación o modificación de información) y / o la disponibilidad (denegación de servicio).

MODELO: Según (Bodeau, Mccollum, y Fox 2018), Un modelo es una representación abstracta de algún dominio de la experiencia humana, utilizado primero, para estructurar el conocimiento, segundo, para proporcionar un lenguaje común para discutir ese conocimiento y tercero para realizar análisis en ese dominio.

ATAQUE, según Magar 2016, El ataque, es la acción de un adversario que instrumentaliza una amenaza con un objetivo específico.

METODOLOGIA, se puede definir como un conjunto de pasos de un proceso para el logro de un objetivo particular, por ejemplo, la metodología para la implementación de un sistema de gestión de seguridad informática.

Las amenazas se pueden describir como “quién” apunta a un “qué”, utilizando un “cómo” para lograr el “por qué”.

“Quién” es la entidad que lleva a cabo el ataque, incluidos los estados nacionales, el crimen organizado y los activistas. "Qué" es el objetivo final del ataque, como datos de tarjetas de crédito o recursos informáticos. "Cómo" es el método por el cual los atacantes llegarán a los datos, como inyección SQL, desbordamientos de búfer o botnet. El "por qué" captura la razón por la que el objetivo es importante para el atacante (Motivación). La mayoría de los modelos de amenazas se centran en el "qué" y el "cómo", ya que esto permite al analista de seguridad identificar vulnerabilidades potenciales en la red o el sistema. El "quién" y el "por qué" a menudo se consideran algo menos importantes, ya que en muchos casos la intención es menos importante que los resultados. La atención se centra en detener el ataque en lugar de determinar quién está realizando el ataque y cuál es su motivación; lo cual es un error ya que perfilar el atacante es muy importante para dimensionar las inversiones que estamos a realizar para disminuir la probabilidad de un ataque. No es lo mismo enfrentarse a un hacker amateur que a una organización criminal, o a todo el poderío de un Estado hostil.

Según ISO 31000 -2018 el Riesgo es el “efecto de la incertidumbre sobre los objetivos “; aquí se combinan dos variables. La primera es la incertidumbre, que es la probabilidad de suceso de un evento o amenaza. La segunda es el efecto o impacto, las consecuencias generadas por la materialización del evento. En otras palabras, es la combinación de la probabilidad de que ocurra un evento y el impacto que acarrea su ocurrencia. En el presente trabajo de investigación, hemos definido el riesgo como una variable cuyo valor se normaliza en un valor entre 0 y 1; donde 0 significa, bien sea que la probabilidad de que se produzca dicho evento es cero, o que el dolor percibido por el impacto es nulo, el valor de 1 de la variable riesgo significa que la probabilidad

de que se materialice la amenaza es altísima, es decir no hay incertidumbre, y su impacto es catastrófico para la organización. El perfil del riesgo del decisor es el que determina su comportamiento frente a un riesgo determinado.

Según NIST IR 8286 A, Apetito de Riesgo y tolerancia del riesgo son dos definiciones que tienden a mencionarse en forma indistinta, para definir el perfil de riesgo de un decisor; pero hay una sutil diferencia entre ambas definiciones; a saber:

- **Apetito de Riesgo**: Es la cantidad de riesgo que una Organización está dispuesta a aceptar con el fin de cumplir con sus objetivos misionales, es una declaración gerencial.
- **Tolerancia al Riesgo**: Es el nivel especifico de riesgo aceptable dentro del apetito de riesgo definido por la alta dirección de una organización; en algunos casos dichos dirección limites pueden estar afectados por restricciones regulatorias o legales.

Según la norma NIST IR 8286 A, El perfil de riesgo se define al nivel gerencial de la organización. Por ejemplo, para una organización global de ventas al detal (minorista), el comité directivo define su apetito de riesgo así: Nuestros clientes asocian confiabilidad con nuestra marca, por lo tanto, debemos minimizar cualquier falla en las páginas web que interactúan con los clientes. Mientras tolerancia al riesgo la definen así: los directores regionales podrán aceptar un tiempo máximo de indisponibilidad del servicio de 4 horas al mes en menos del 5% de los clientes, dependiendo de la región. El apetito de riesgo y la tolerancia al riesgo están relacionados, pero son distintos, de manera similar a la relación que existe entre las actividades de gobierno corporativo y las actividades de gestión o dirección de la gerencia general. Mientras que las declaraciones de apetito por el riesgo definen la orientación general del riesgo, las declaraciones de tolerancia al riesgo definen la aplicación específica de esa orientación. Esto significa que las declaraciones de tolerancia al riesgo son siempre más específicas que las correspondientes declaraciones de apetito

de riesgo. Juntas, estas declaraciones de apetito por el riesgo y de tolerancia al riesgo representan los límites del riesgo, ayudan a comunicar las expectativas de riesgo, en otras palabras, definen el perfil de riesgo de una organización y mejoran el enfoque de los esfuerzos de gestión del riesgo, es decir, definen la forma como se comportan dos organizaciones diferentes frente al mismo riesgo.

## **1.2.** Definición de Modelado de Amenazas

Antes de desarrollar la investigación en primera medida se hace una revisión bibliográfica de diferentes documentos para definir el modelamiento de amenazas ya que es un concepto que ha tenido una gran variedad de definiciones y para acercarnos a una más exacta a continuación se cita algunos autores que definen este término:

(Castellaro, Romaniz & Ramos 2013) definen el modelamiento de amenazas como una herramienta que evalúa los riesgos de una aplicación durante la etapa de desarrollo. Es un proceso de análisis de riesgo estructurado que identifica amenazas de un software y cuantifica los riesgos a los que está expuesto.

(Barba Olivares 2017) afirma que el modelamiento de amanezcas es un instrumento que mejora el desarrollo del diseño de un programa pues ayuda que el software posea protecciones en contra de los ciberataques. Es fundamental que las personas que participa en la creación del software desarrollen dos posturas la de defensor y la de atacante. La parte que es defensora debe analizar que vulnerabilidades tiene el software para después crear mecanismos que garantice la seguridad del sistema y la parte atacante intenta comprender los posibles ataques que se pueden realizar en contra del software.

(Castellaro et al. 2016) señalan que el modelamiento de amenazas es una herramienta que tiene como propósito identificar y planificar estrategias para mitigar las amenazas cibernéticas.

Básicamente esta técnica busca que varios actores como desarrolladores, tester, gerencia, administradores de sistemas, consultores y auditores participe en la construcción del sistema para que analice la estructura y examine las vulnerabilidades del software.

(Bodeau et al. 2018) dicen que el modelamiento de amenazas es un proceso que evalúa las vulnerabilidades a los que está expuesto un sistema con el objeto de encontrar amenazas que ponen en peligro la información de la organización por medio, de este análisis se desarrolla medidas para manejar el riesgo, técnicas como identificación de puntos de entrada, fronteras de privilegios y árboles de amenazas que permite reducir las amenazas de ataques cibernéticos.

(Pols 2017) manifiesta que el modelamiento de amenazas es una técnica de ingeniería que tiene como finalidad indicar los posibles ciberataques que podría enfrentar el sistema para luego mejorarlos.

(Bodeau y Graubart 2013) indican que el modelamiento de amenazas es un proceso que analiza las diferentes amenazas a la que puede estar expuesto un sistema o aplicación tiene como objeto preparar mecanismos de defensa y establece medidas de seguridad durante las etapas de creación del software para hacerlo más seguro de los ataques.

(Barrios, Rio, y Esguerra Estarita 2006) sostienen que el modelamiento de amenazas es un proceso que tiene como función analizar las vulnerabilidades que tiene un software o un producto. Este análisis sirve para averiguar los puntos débiles que tiene el sistema para después implementar códigos de seguridad.

Aunque no exista un concepto exacto de modelamiento de amenazas, podemos decir que todas las definiciones hacen referencia que es un proceso metodológico que en su fase inicial hace un reconocimiento del objetivo, estudia comportamientos y analiza las vulnerabilidades de la víctima y con base a esta información los ciberdelincuentes diseñan el ataque, escogen el exploit,

el payload y la forma de acceder a los sistemas tele informáticos de la víctima, posteriormente una vez tienen acceso inician un proceso de post-explotación donde comienza a extraer información vital de la víctima como por ejemplo tabla de users y passwords, hace movimientos laterales dentro del sistema con el fin de tener control de todo el sistema. El reto del atacante es hacer todo este proceso generando el menor "ruido" posible dentro de los sistemas de la víctima, para evitar ser detectado. Uno de los objetivos del modelamiento de amenazas es diseñar una arquitectura optima de ciberseguridad partiendo desde el punto de vista del atacante, del tipo de atacante, de tal forma que permita detectar en forma temprana un posible ataque, escogiendo los mecanismos de protección adecuadas que maximicen la relación costo/beneficio, tal que disuada al atacante o por lo menos incremente el tiempo y los recursos gastados en acceder al sistema en forma fraudulenta. Otro de los objetivos es poder calcular la probabilidad de un escenario de ataque y de esta forma poder estimar el riesgo.

Para que se puede llevar a cabo un ataque se deben estar presentes tres condiciones:

1. El defensor debe tener vulnerabilidades o debilidades en su sistema.
2. El agente de amenaza (Atacante) debe tener suficientes recursos disponibles (Técnicos y/o económicos) para explotar las vulnerabilidades del defensor. Esto se conoce como capacidad.
3. El atacante debe creer que se beneficiarán al realizar el ataque. La expectativa de beneficio impulsa la motivación.

La condición 1 depende completamente del defensor.

La condición 2 depende principalmente del atacante, pero la cantidad de recursos utilizados para realizar el ataque, depende de que tan fácil se lo permita el defensor. Diferentes agentes de amenaza tienen diferentes capacidades.

La condición 3 involucra principalmente al atacante. Representa la motivación para llevar a cabo el ataque. El defensor puede tener un papel si sus acciones provocan que un agente de amenaza realice un ataque.

El agente de amenaza y el defensor interactúan para determinar conjuntamente si ocurre un ataque. El análisis de ataque adecuado requiere que examinemos las tres condiciones para predecir el comportamiento de los adversarios y la probabilidad de que ocurra un ataque. Comprender estos factores también proporciona información sobre formas efectivas de prevenir ataques.

### **1.3.** Caracterización del atacante y de un ataque.

Es importante en este parte del documento caracterizar los atacantes y categorizar los diferentes tipos de ataque, según (Magar 2016):

Atacante (Adversario).

El adversario como se ilustra en la Figura 1 tiene las siguientes características:

- Tipo: esta categoría identifica los diversos tipos de atacantes cibernéticos
- Motivación: La motivación es un indicador importante tanto del nivel de malevolencia como de la probabilidad de intento. La motivación del adversario se dividió en motivaciones hostiles y no hostiles
- Compromiso: El compromiso del adversario, se utiliza para describir la voluntad de la amenaza
- Recursos: Describe la Capacidad con los que cuenta el atacante,


*Figura 1. Categorización del Atacante - Traducción propia. Magar (2016)*

Un atributo del adversario es una característica discreta o propiedad distintiva de una amenaza. Las características combinadas de una amenaza describen la voluntad y la capacidad de la amenaza para perseguir su objetivo. Tal como se puede observar en la Figura 1, Hay varios atributos que permiten clasificar a una atacante, a saber: el tipo, la motivación, el compromiso y los recursos. En el ámbito de este trabajo de investigación es importante aclarar dos grupos de atributos, los relacionados con el compromiso, que describen la determinación del adversario, y con los recursos, que describen las capacidades del adversario.

Existen los siguientes tres atributos en la familia de compromiso:

- Intensidad: el atributo Intensidad de una amenaza describe la diligencia o determinación perseverante de una amenaza en la búsqueda de su objetivo. Este

atributo también incluye la pasión que siente el atacante por su objetivo. La intensidad es una medida de qué tan lejos está dispuesto a llegar un atacante y qué está dispuesto a arriesgar para lograr su objetivo. Las amenazas con mayor intensidad, por lo tanto, se consideran más peligrosas debido a su ambición motriz en la búsqueda de un objetivo;

- Sigilo: el atributo Sigilo de una amenaza describe la capacidad del atacante para mantener el nivel necesario de secreto durante la consecución de su objetivo. El mantenimiento del secreto puede requerir la capacidad de ocultar algunos o todos los detalles sobre la organización de la amenaza, incluido su objetivo, su estructura o sus operaciones internas. Un mayor nivel de sigilo permite que un atacante oculte sus actividades previstas, así como su estructura interna, del mundo exterior. Esto dificulta la recopilación de inteligencia y las medidas preventivas para contrarrestar o prevenir los ataques de la amenaza; y

- Tiempo: el atributo Tiempo de una amenaza cuantifica el período de tiempo que un atacante es capaz de dedicar a la planificación, el desarrollo y la implementación de métodos para alcanzar un objetivo. En el caso de un ataque cibernético o cinético, incluye el tiempo necesario para todos los pasos de implementación hasta la ejecución real. Cuanto más tiempo un atacante esté dispuesto y pueda dedicarse a preparar un ataque, más potencial tiene la amenaza de impactos devastadores.

Hay tres atributos en la familia de recursos:

- Personal Técnico: el atributo Personal Técnico de una amenaza cuantifica el número de miembros del grupo que un atacante es capaz de dedicar a la construcción y despliegue de la capacidad técnica en pos de su objetivo. El personal técnico incluye solo a los miembros del grupo con tipos específicos de conocimientos o habilidades, como cinético o cibernético, y aquellos directamente involucrados con la fabricación real de las armas del grupo. Una amenaza con un nivel más alto de Personal Técnico tiene un mayor potencial de diseño y desarrollo innovadores, lo que permite la posibilidad de nuevos métodos para alcanzar una meta que puede que no haya estado disponible en el pasado. Además, un nivel más alto de personal técnico también acelera el diseño y desarrollo de los planes de ataque de una amenaza;

- Conocimiento: el atributo Conocimiento de una amenaza define el nivel de competencia teórica y práctica del atacante y la capacidad de emplear esa competencia en la búsqueda de su objetivo. El conocimiento también incluye la capacidad de un atacante para compartir información, adquirir capacitación en una disciplina necesaria y mantener un programa de investigación y desarrollo. Sin embargo, este atributo no incluye ninguna competencia encontrada o comprada fuera de la organización del atacante. Este atributo incluye conocimientos relacionados con la capacidad ofensiva y defensiva dentro de la categoría. Cuanto mayor sea el conocimiento de un atacante en su conjunto, más capacidad tiene una amenaza para perseguir su objetivo con menos

recursos y en menos tiempo. Además, el conocimiento de un atacante proporciona un medio para diferenciar entre amenazas cibernéticas, cinéticas o híbridas; y

- Acceso: el atributo Acceso de una amenaza define la capacidad de una amenaza para colocar a un miembro del grupo dentro de un sistema restringido, ya sea a través de medios cibernéticos o cinéticos, en la búsqueda del objetivo. Se considera sistema restringido a cualquier sistema, ya sea cibernético o físico, donde el acceso se otorga en función de privilegios o credenciales. La característica de Acceso detalla la capacidad de un atacante para infiltrarse en un sistema restringido, ya sea a través de un miembro del grupo privilegiado, el chantaje y la coacción de un transeúnte inocente o la corrupción de una red o sistema informático poco protegido. La infiltración de una amenaza puede producir una amplia variedad de efectos: la necesidad de menos recursos para lograr un objetivo, la implementación de un esquema a largo plazo de manipulación de productos o un mayor nivel de conocimiento íntimo de un objetivo.

ATAQUE.

El ataque, según Magar (2016) es la acción de un adversario que instrumentaliza una amenaza con un objetivo específico, como ilustrado en la Figura 2, tiene las siguientes características:

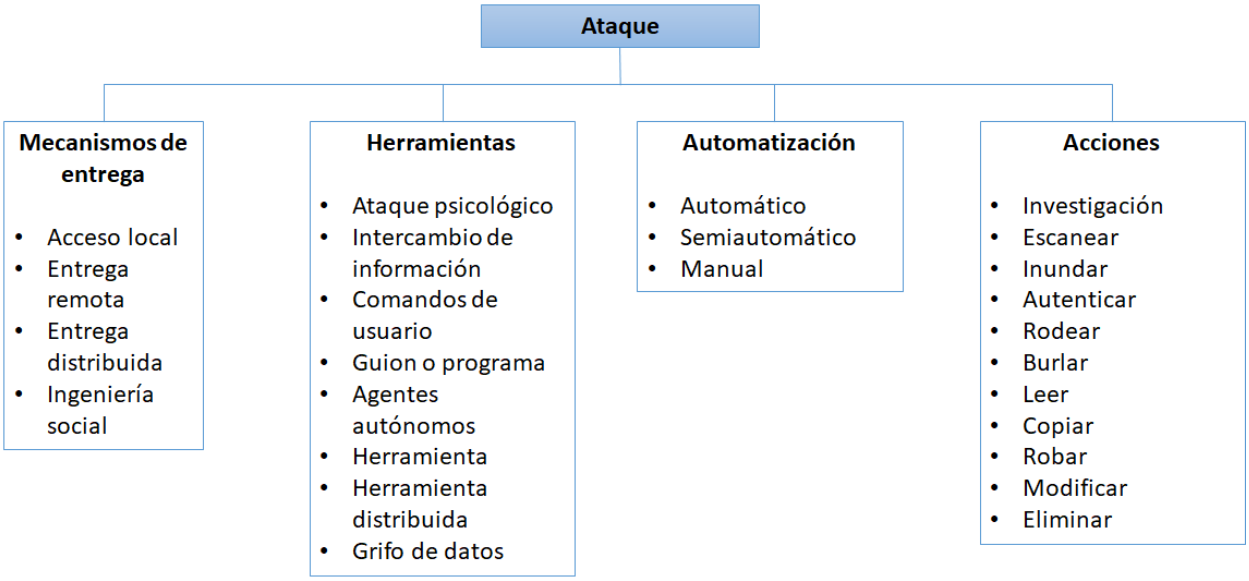



*Figura 2. Caracterización de un ataque. - Traducción propia. Magar (2016)*

- Mecanismos de Entrega – El concepto de mecanismos de entrega, que se refiere al medio con el cual el ataque es entregado, Sin embargo, parece existir un poco de confusión entre los mecanismos de entrega y las herramientas: por consecuencia, el autor ha intentado definir lo siguiente para los mecanismos de entrega:
    - Acceso Local – Para implementar un ataque, es necesario tener acceso local. Este es el caso para un ataque físico o la implementación de un keylogger físico;
    - Entrega Remota – El ataque puede ser realizado de manera remota. Entrega remota incluye archivos adjuntos en correos electrónicos, intentos de penetración directa, etc.;
    - Entrega Distribuida – El ataque debe ser distribuido entre varios sistemas. Entrega distribuida incluye DDoS, spam, etc.;
    - Ingeniería Social – Ingeniería social hace referencia al ataque que requieren interacción personal sea por teléfono o personalmente;

- Herramientas – Herramientas son los medios utilizados para explotar la vulnerabilidad de un computador o de una red.
- Automatización. Clasificación por grado de autonomía - Durante la preparación del ataque, el atacante necesita localizar posibles máquinas agentes e infectarlas con el código de ataque. Especialmente definida para categorizar los diferentes tipos de Ataque de denegación de servicios distribuida, DDoS por sus siglas en Ingles, Basándose en el grado de automatización del ataque, la taxonomía distingue entre ataques DDoS manuales, semiautomáticos y automáticos. Sólo los primeros ataques DDoS pertenecen a la categoría manual. El atacante escaneaba las máquinas remotas en busca de vulnerabilidades, entraba en ellas e instalaba el código de ataque, y luego ordenaba el inicio del ataque. Todas estas acciones pronto se automatizaron, lo que llevó al desarrollo de los ataques DDoS semiautomáticos, la categoría a la que pertenecen la mayoría de los ataques contemporáneos. Los ataques DDoS automáticos automatizan además la fase de ataque, evitando así la necesidad de comunicación entre el atacante y las máquinas agentes.

- Acciones – Acciones son un paso dado por un usuario o proceso para llegar a un resultado.

### **1.4.** Tipos de Análisis de Modelamiento de Amenazas

Básicamente, modelar amenazas podría considerarse como un intento estructurado de identificar amenazas cibernéticas basadas en sus objetivos, en la identificación de vulnerabilidades en la víctima, y de esta forma, proporcionar técnicas de mitigación (contramedidas) que aborden las amenazas identificadas. Existe una amplia variedad de técnicas para modelar amenazas y ataques que se pueden clasificar en tres categorías generales, a saber, centradas en el atacante, centradas en el sistema y centradas en los activos en función de su comportamiento y estrategia de

identificación. Según (Esmeailli y Esterabadi 2019), los tipos de análisis de modelamiento de amenazas son (Ver Figura 3):

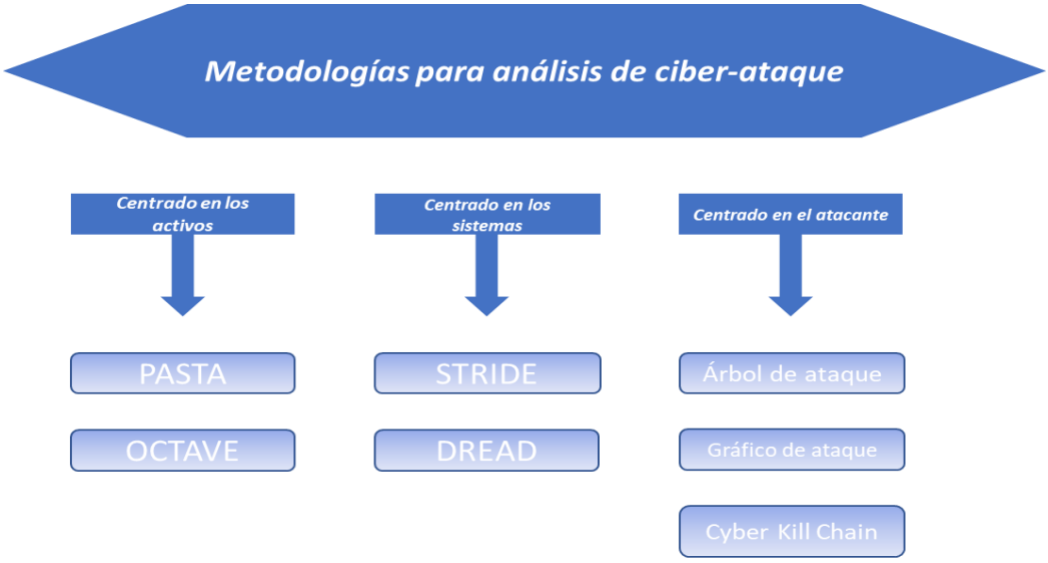



*Figura 3. Clasificación de Metodología para modelamiento de amenazas. Esmeailli y Esterabadi (2019)*

**1.4.1.** Análisis en centrado en el atacante. En esta clase de análisis se analiza el comportamiento del atacante y el diseñador o programador debe determinar ¿qué quiere el atacante? y ¿cómo puede atacar? Una vez se conteste estas preguntas se implementa medidas de seguridad (Quiroga, 2018).

Según (Esmaeili y Esterabadi 2019) un modelamiento centradas en el Atacante se centra en las capacidades, motivaciones y objetivos del atacante y la forma en que se pueden lograr. Ha sido considerado por algunos de los modelos conocidos como TARA (Análisis de amenazas y evaluación de riesgos, por su significado en inglés) de Intel, Grafos de ataque, Árbol de ataques y Cyber Kill Chain.

**1.4.2.** Análisis centrado en el software (Sistemas).

Este enfoque, también conocido como "centrado en el sistema " o "centrado en el diseño", se centra en un software que se está desarrollando o un sistema que se está construyendo. Este modelo comienza desde la fase de diseño de un software o sistema e investiga diferentes amenazas posibles contra cada componente del sistema a través de todo el proceso de desarrollo. El enfoque centrado en el sistema se usa comúnmente en diferentes sistemas de información y se ha convertido en un estándar legítimo en el alcance de los sistemas de información. Dos de los modelos de amenazas más conocidos Centrados en el Sistema son STRIDE, que ha sido desarrollado por Microsoft y DREAD.

1.4.2.1 STRIDE.

Es un enfoque de modelado de amenazas Centrado en el Sistema, propuesto por Microsoft en 1999, comúnmente utilizado en su propio proceso de desarrollo de productos, así como en muchas otras industrias, incluida la automotriz [12]. Este método es compatible con algunos de los esquemas de software seguro más destacados, tales como el OWASP. STRIDE es un acrónimo inducido por diferentes clasificaciones de amenazas que pueden poner en peligro el sistema en consideración, estas clasificaciones son las siguientes:

- Engañar (Spoofing): Los atacantes obtienen acceso ilegítimo a información confidencial al manipular su identidad. Esto amenaza la confidencialidad del sistema según la tríada de la CIA (por sus siglas en ingles Confidentiality, Integrity, Availability)

- Manipulación (Tampering): Manipular los datos que atraviesan canales de comunicación o almacenados en una base de datos. Esto se considera una violación de la integridad según la tríada de la CIA.

- Repudio (Repudiation): La incapacidad de rastrear un ataque para identificar al atacante potencial
- Divulgación de Información (Information Disclosure): Acceso no autorizado del atacante a los datos en tránsito o a una base de datos.
- Negación de Servicio (Denial of Service): Cualquier intento del atacante para interrumpir el funcionamiento normal del sistema y dejarlo fuera de servicio.
- Elevación de Privilegios (Elevation of privilege): El atacante obtiene acceso no autorizado a un sistema que le permite realizar operaciones críticas al obtener privilegios de la raíz del sistema.

1.4.2.2 DREAD.

El método DREAD, que también es un modelo de Microsoft, puede utilizarse durante el proceso de evaluación de riesgos. Este método realmente influye en el proceso de cuantificación, priorización y, en consecuencia, categorización de los riesgos asociados. Se compone de cinco categorías diferentes para el análisis de riesgos. DREAD es un acrónimo derivado de las letras iniciales de cada una de estas cinco categorías, según son ellas:

Daño potencial (Damage potential): Cuantificar el alcance de un daño derivado de la explotación de una vulnerabilidad conocida.

Reproducibilidad (Reproducibility): Clasificación de la probabilidad de la explotación exitosa de una vulnerabilidad conocida.

Explotabilidad (Exploitability): Cuantificar los esfuerzos que un atacante necesita para la explotación exitosa de una vulnerabilidad conocida. Esto también podría considerarse como una condición previa que un atacante podría necesitar para realizar un ataque exitoso.

Usuarios Afectados (Affected users): Un valor que representa el número de instancias instaladas del sistema que se verían afectadas si una amenaza está ampliamente disponible.

Descubrimiento (Discoverability): Este factor especifica la probabilidad de que investigadores externos de seguridad, piratas informáticos, etc. puedan encontrar una vulnerabilidad abierta.

DREAD valora cada una de las cinco categorías antes mencionadas en una escala de calificación de 0-10. A medida que la tasa crece de 1 a 10, representa una mayor probabilidad de ocurrencia con un mayor potencial de daño. En consecuencia, el riesgo general para el sistema también podría calcularse con base en la fórmula proporcionada que se muestra a continuación: Esta fórmula utiliza el promedio de los valores de las cinco categorías de DREAD. Trivialmente, el riesgo calculado siempre reside entre 0-10, donde un valor más alto representa un riesgo más alto para el sistema.

$$Risk\_DREAD = \frac{\textbf{D}\text{amage} + \textbf{R}\text{eproducibility} + \textbf{E}\text{xploitability} + \textbf{A}\text{ffected Users} + \textbf{D}\text{iscoverability}}{5}$$

Alemán Novoa y Rodríguez Barrera 2015) señalan que este tipo de análisis (STRIDE & DREAD) se examina las vulnerabilidades que tiene el software para averiguar si efectivamente el sistema cuenta con la correcta protección.

Es importante recordar que para que un software sea seguro debe garantizar la confidencialidad, la integridad, la disponibilidad, la responsabilidad y la no repudiación.

### 1.4.3. Análisis centrado en los activos.

El enfoque centrado en los activos se centra en la información o los recursos objetivo de un sistema que un atacante intenta comprometer. Este enfoque es más común que el método centrado en el atacante. Sin embargo, los modelos que utilizan este enfoque se consideran que

consumen mucho tiempo y recursos, ya que necesitan más tiempo y más recursos para modelar diferentes amenazas contra el sistema destino. Los modelos centrados en activos más conocidos son PASTA y OCTAVE.

#### 1.4.3.1 PASTA.

(Process for Attack Simulation and Threat Analysis - Proceso para la simulación de ataque y el análisis de amenazas) es una estrategia que busca proporcionar un proceso de simulación de ataque junto con un esquema de análisis de amenazas cibernéticas y, en última instancia, reducir los riesgos de delitos cibernéticos derivados de estas amenazas mediante el uso de estrategias de mitigación. Como se muestra en la Figura 5, para alcanzar los objetivos anteriores, Según Ucedaveles y Morana (2015) PASTA realiza siete pasos consecutivos en aras del análisis de amenazas y riesgos. Al seguir estas siete etapas, cualquier empresa puede caracterizar los factores de mitigación necesarios para abordar los riesgos asociados con las amenazas cibernéticas y los consiguientes ataques a una aplicación. PASTA combina el análisis de amenazas a nivel de sistema o de aplicación con objetivos comerciales, análisis de negocios y cumplimiento. A pesar del hecho de que es posible adaptar este método a diferentes entornos, dado que este modelo se enfoca en los accionistas y el impacto comercial de las amenazas de seguridad, consideramos que es principalmente compatible con los modelos comerciales en lugar del proceso de desarrollo de productos.


*Figura 4. Metodología PASTA para análisis de Amenazas y Riesgos. Esmeailli y Esterabadi (2019)*

1.4.3.2 OCTAVE.

- OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation,) Evaluaciones de amenazas a las operaciones críticas, activos y vulnerabilidades, según Alberts & Dorofee (2003) es una evaluación estratégica basada en el riesgo y una técnica de planificación para la seguridad Se considera como un enfoque

autodirigido. A diferencia de la mayoría de las evaluaciones de un sistema que se enfoca en riesgos tecnológicos y problemas tácticos, OCTAVE destaca el riesgo organizacional y se enfoca en problemas estratégicos y prácticos. Con el fin de abordar los requisitos de seguridad, OCTAVE considera a toda la organización y a las personas tanto de la tecnología de la información como de otros departamentos operativos. De acuerdo con la Figura 6, OCTAVE pretende ayudar a las organizaciones a equilibrar tres aspectos clave de cualquier infraestructura de red, a saber, riesgos operativos, prácticas de seguridad y tecnología.

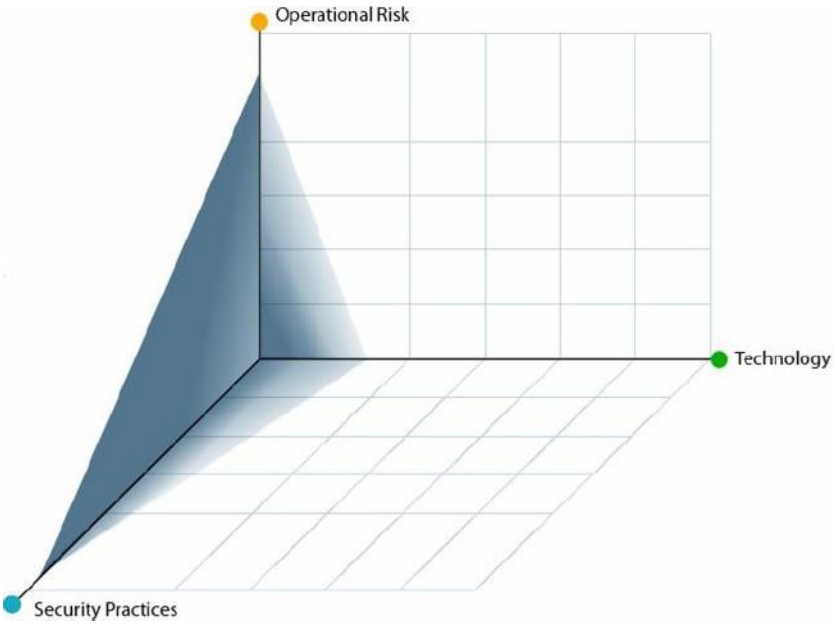



*Figura 5 Tres aspectos clave equilibrados por OCTAVE. Falta referencia*

OCTAVE es un enfoque de evaluación basado en activos. Equipos que realizan un análisis en un sistema o infraestructura específicos:

1. Identificar activos críticos relacionados con la información (por ejemplo, información y sistemas).

2. Enfocar las tareas de análisis de riesgos en los activos que se evalúan como los más críticos para la organización.
3. Considerar las vulnerabilidades (tanto organizativas como tecnológicas) de los activos críticos, las amenazas contra esas vulnerabilidades y la relación entre los activos asociados
4. Evaluar los riesgos desde el punto de vista operativo: cómo se utilizan los activos en el negocio de la organización y cómo están en riesgo debido a las amenazas de seguridad.
5. Crear un mecanismo de defensa práctico para la mejora organizacional junto con una estrategia de mitigación para reducir el riesgo relacionado con los activos críticos.

## **1.5.** Tipos de Metodologías de Modelamiento de Amenazas centradas en el atacante

Las metodologías de modelamiento de amenazas centradas en las atacantes más conocidas son:

1.5.1. Árbol de Ataques. (Schneiera 2019) afirma que la metodología de árbol de ataque es una representación gráfica o un diagrama conceptual en forma de árbol que permite conocer las posibles vías por las que puede perpetrarse un ataque (escenarios). Con base a esta información las organizaciones saben cómo defenderse en caso que se presente un ciberataque y el diseñador del software crea un sistema capacitado para enfrentar todas estas probabilidades de ataques. Para elaborar un árbol de ataque debe ponerse en el lugar del atacante y pensar como el atacante podría atacar el sistema. Según (Estrada 2017) los elementos de un árbol de ataque son:

*1.5.1.1. Nodo raíz.* El nodo raíz está ubicado en la parte superior del árbol y se representa a través de un circuló que simboliza el objetivo del atacante (Ver Figura 6). Un ejemplo de objetivo de ataque es conseguir acceso al servidor para obtener información de la compañía.


*Figura 6 Símbolo de objetivo de ataque. Fuente: Elaboración propia del autor.*

*1.5.1.2. Nodos.* Los nodos hojas representan acciones que se llevan a cabo para perpetrar el ataque y tiene una forma cuadrada. Estos nodos hojas captan la interacción del atacante con la víctima. Estos nodos se completan con diferentes datos tales como: descripciones de los recursos técnicos y económicos que el atacante requiere para realizar la acción, así como el impacto de la víctima y los beneficios para el atacante resultante de esa interacción. Un ejemplo de nodo es el que se muestra en la Figura 7.

| NODO: EXPLORAR VULNERABILIDAD | | |
|---|---|---|
| RECURSOS ATACANTE | COSTOS ATAQUE | Medio |
| | HAB TECNICA | Alto |
| GANANCIA ATACANTE | Ninguna | |
| IMPACTO VICTIMA | Ninguno | |

*Figura 7 Ejemplo de nodo hoja. Fuente: Elaboración propia del autor.*

*1.5.1.3. Relaciones.* (Estrada 2017) afirma que las relaciones hacen referencia de como las acciones se conectan unas con otras para lograr el objetivo del ataque y se representa por medio de puertas lógicas. Existe tres tipos de relaciones:

*1.5.1.3.1. Relación secuencial.* No se puede hacer la siguiente acción sino realiza la anterior y se representa a través de una flecha (Ver Figura 8).

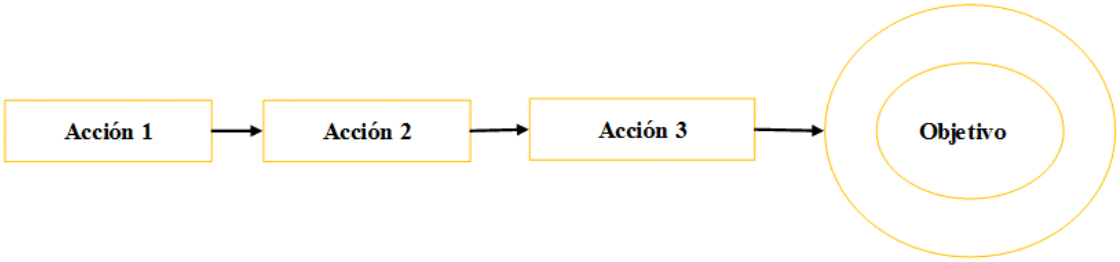



*Figura 8 Relación secuencial. Fuente: Elaboración propia del autor.*

*1.5.1.3.2. Relación AND.* Es posible que para realizar la siguiente acción deba cumplir con las acciones previas. Con la relación AND se puede observar las acciones que se tiene que desarrollar (Ver Figura 9). El nodo AND, describe un proceso.

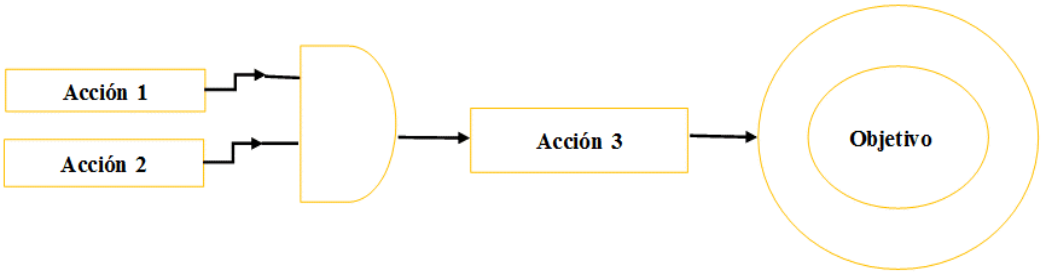



*Figura 9 Relación AND. Fuente: Elaboración propia del autor.*

*1.5.1.3.3. Relación OR.* Es posible que se pueda pasar a la siguiente acción siempre y cuando cumpla una de las acciones posteriores ya que no es necesario cumplir con todas para pasar a la siguiente acción (Ver Figura 10). El nodo OR, describe alternativas para un escenario de ataque.

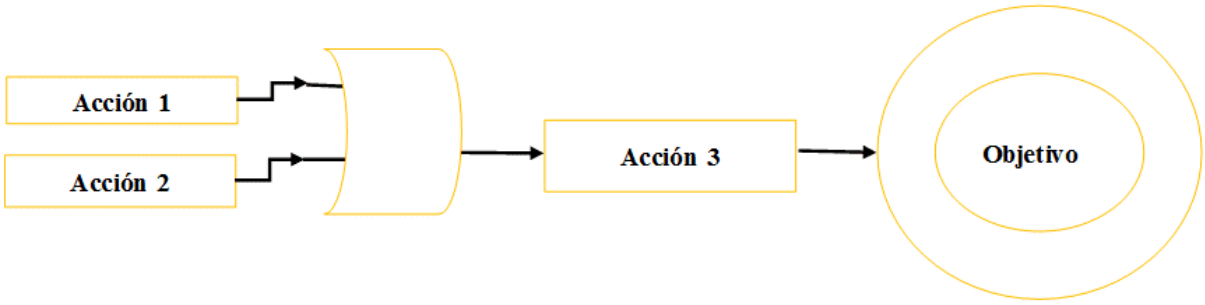



*Figura 10 Relación OR. Fuente: Elaboración propia del autor.*

1.5.2. Grafo de Ataques.

Según Esmeali & Esterabadi (2019), los grafos de ataque son una poderosa técnica de modelado utilizada para representar las rutas a través de las cuales se pueden realizar ataques para alcanzar un objetivo malicioso. En general, los nodos en un gráfico de ataque representan los estados del sistema mientras ocurre un ataque. Estos nodos se clasifican en estado inicial, estados intermedios y estado objetivo. Los bordes, por otro lado, representan las acciones tomadas por el atacante para transitar de un estado a otro hasta alcanzar la meta final.

Por ejemplo, como se muestra en la Figura 11, considere un escenario en el que el atacante (Eve) intenta obtener el acceso raíz en una máquina de destino (Alice) mediante el uso de vulnerabilidades en los otros hosts (Bob y Charlie) del sistema. Hay un puerto abierto en la máquina de Charlie con una vulnerabilidad explotable de forma remota. Además, el cortafuego solo permite que pase el tráfico destinado a la máquina de Bob y se elimina el resto del tráfico. Bob tiene la dirección de red de Alice y puede comunicarse libremente con ella. Además, la máquina de Alice no tiene una seguridad estricta, es decir, la función de inicio de sesión remoto y el servicio FTP son vulnerables y el acceso a la raíz también se puede obtener explotando el desbordamiento de búfer.

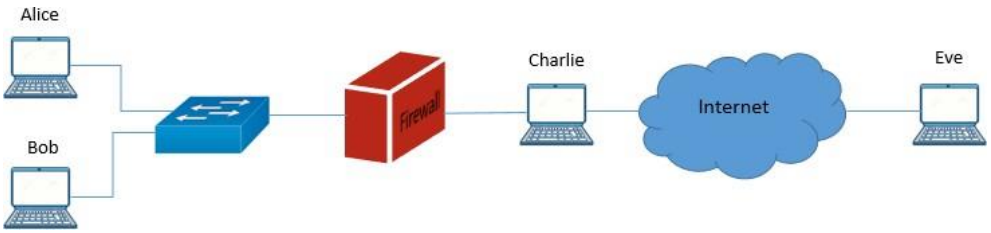



*Figura 11 Escenario simple para un atacante que aumenta sus privilegios. Esmeali & Esterabadi (2019)*

La figura 12 representa el gráfico de ataque correspondiente al escenario anterior. El atacante que explota la vulnerabilidad asociada con el puerto abierto, obtiene acceso remoto a la máquina de Charlie. Una vez allí, el atacante puede comunicarse con Bob, ya que el firewall solo permite el tráfico entrante destinado a su máquina. Después de comprometer la máquina de Bob, el atacante puede usar la función de inicio de sesión remoto o implementar un nuevo archivo de host usando FTP para acceder a la máquina de Alice. Finalmente, el atacante explota el desbordamiento de búfer para obtener el acceso raíz.

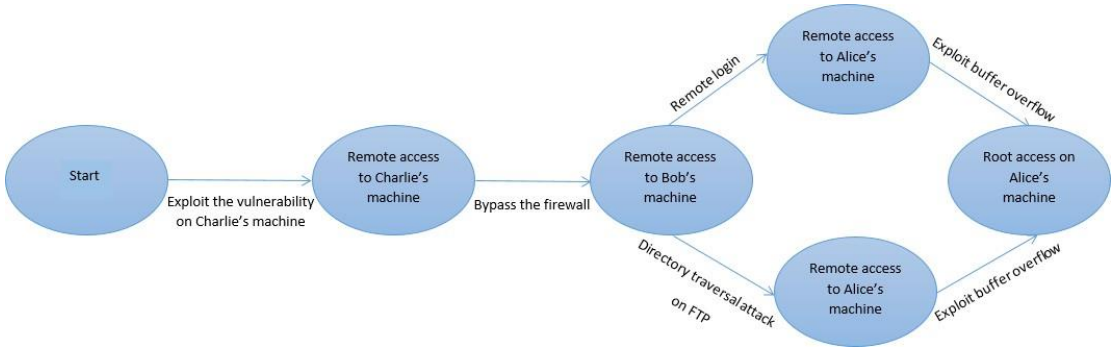



*Figura 12 Modelo de gráfico de ataque para el escenario de escalada de privilegios. Esmeali & Esterabadi (2019)*

1.5.3. Ciclo de Vida de Amenaza. Es un proceso que describe las etapas de un ataque. Con base a esta metodología permite a las organizaciones o a las instituciones diseñar políticas de

seguridad para proteger el sistema de ataques cibernéticos. (Ramírez 2017) dice que el ciclo de vida de amenaza también es conocido como cadena de ciberataque o ciclo de vida de ataques cibernéticos o Cyber Kill Chain. El ciclo de vida de amenaza es un término usado por los militares para señalar cuáles son los pasos que utiliza el enemigo o un ciberdelincuente a la hora de atacar un determinado objetivo. Para detectar, detener, interrumpir y preparar un ciberataque es importante conocer el ciclo de vida de la amenaza para poder desarrollar e implementar mecanismos de protección que garantice la mayor seguridad posible al sistema. (Jiménez 2020) manifiesta que esta metodología fue usada por Lockeed Martin para indicar los pasos o fases de un ataque con el propósito de saber cómo interactúa el atacante y de esta manera tomar decisiones a tiempo para romper la cadena o bloquear el ciberataque. Cada ataque genera una serie de huellas que ayuda a los expertos en ciberseguridad y ciberdefensa aprender a comprender como los cibercriminales usan estas herramientas para realizar ataques, esto permite diseñar mecanismos de defensa cada vez más efectivos. Según L Martin (2015) el ciclo de vida de amenaza está conformado por siete pasos que a continuación se explican cada uno (Ver Figura 13):

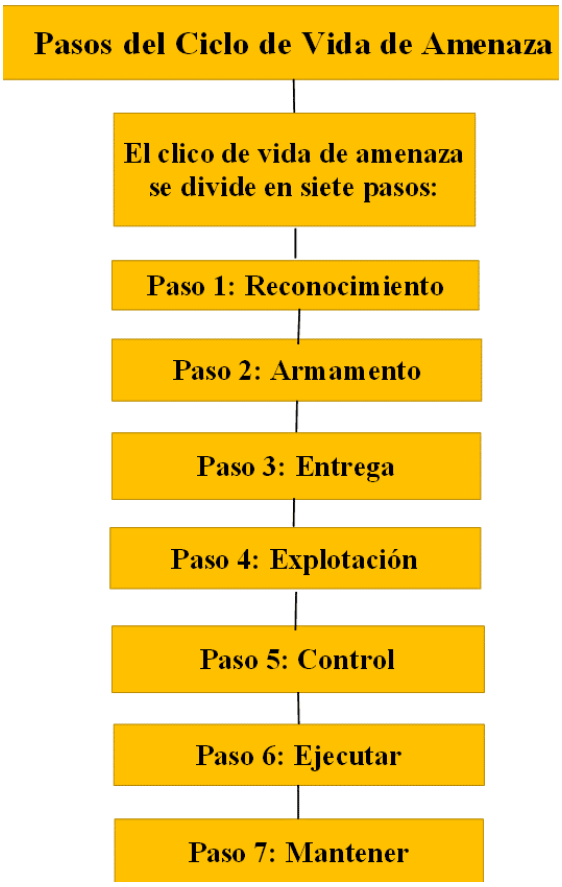



*Figura 13 Pasos del ciclo de vida de amenazas. Fuente: Elaboración propia del autor.*

*1.5.3.1. Paso 1: Reconocimiento.* En este primer paso el atacante recolecta información sobre el objetivo, por lo tanto, analiza la organización en aspectos como bases de datos, redes sociales, hace interacciones por correo electrónico e incluso verifica si la empresa usa algún tipo mecanismo de seguridad para proteger el sistema en caso que se presente un ataque.

*1.5.3.2. Paso 2: Armamento.* En este segundo paso el atacante desarrolla un mecanismo o una herramienta como un malware para lograr el objetivo.

*1.5.3.3. Paso 3: Entrega.* En este tercer paso el atacante envía a la organización un virus informático como bots, ransomware o malware.

*1.5.3.4. Paso 4: Explotación.* En este cuarto paso se ejecuta el ataque y se explota una vulnerabilidad del sistema para instalar y activar el malware para infectar el servidor de la organización.

*1.5.3.5. Paso 5: Control.* En este quinto paso el atacante ya tiene control del sistema de la organización, puede tomar capturas de pantalla, obtener documentación confidencial, instalar programas, acceder a las bases de datos que contiene nombres, direcciones, correo electrónico entre otra información personal de los clientes y trabajadores de la compañía.

*1.5.3.6. Paso 6: Ejecutar.* En este sexto paso el atacante ejecuta el plan y logra los objetivos propuestos.

*1.5.3.7. Paso 7: Mantener.* En este séptimo paso el atacante mantiene una presencia a largo plazo en el sistema para obtener toda la información posible de la organización.

Conclusión Capitulo 1.

Después de esta amplia presentación de metodologías de análisis de amenazas, finalmente seleccionamos el árbol de ataque ( Ver Figura 14 ) como la metodología que nos permite modelar un ataque en forma flexible, ya que permite describir el nivel detalle del ataque acorde al objetivo buscado, permite calcular el riesgo de diferentes para cada escenario de ataque, es un método fácil de usar extremadamente visual, lo cual facilita la presentación en auditorios de decisión donde no se tiene un conocimiento especializado, pero aprueban el presupuesto de inversión; además es el único método encontrado en este trabajo de investigación , que permite modelar victimas con diferentes perfiles de tolerancia al riesgo y medir su efecto en la toma de decisiones de inversiones en ciberseguridad. Las Metodologías STRIDE y DREAD están hechas principalmente para prevenir amenazas en el desarrollo de productos de software; mientras las metodologías de PASTA

y OCTAVE son un marco de referencia para la implementación de un sistema de gestión de seguridad a nivel empresarial, similar a ISO 27032 o NIST 880-30 SP.

| CRITERIOS | Arbol de ataque | Grafos de Ataque | CKC |
|---|---|---|---|
| Calculo Riesgo ( Impacto * Prob ) | SI | si | NO |
| Flexibilidad ( nivel Abstracion ) | SI | No | SI |
| Descripcion Ataque | SI | si | SI |
| Perfil Atacante | SI | NO | NO |
| Perfil Victima | SI | NO | NO |
| Modelar Contramedidas | SI | si | SI |
| Facilidad Uso / Visual | SI | NO | NO |

*Figura 14 Criterios de escogencia Modelamiento de Amenazas. Elaboración propia*

## 2. CAPITULO II

### **2.1.** Ataques Cibernéticos que ha Sufrido las Universidades

En este apartado se explica los problemas que enfrenta las universidades por la falta de un sistema de ciberseguridad, se trata los informes de ciberataques, los tipos de ataques cibernéticos más comunes en las instituciones educativas, por último, se cita algunos casos de ataques informáticos que ha sufrido las diferentes universidades en Colombia.

### **2.2.** Problemas que Enfrenta las Universidades por la Falta de un Sistema de Ciberseguridad

Vivimos en una sociedad en la que casi todas las actividades cotidianas que realiza el ser humano como económicas, sociales, culturales y políticas requiere del internet para poder desarrollarlas. Las tecnologías de la información y la comunicación revoluciono la manera de interactuar con el mundo pues, permite a las personas trabajar, hacer negocios, estudiar, intercambiar ideas, compartir información, subir fotos, videos, pagar facturas, jugar juegos, participar en discusiones políticas, sociales, culturales y económicas, enviar correos electrónicos, comprar en línea y facilita la comunicación entre los individuos a un bajo costo sin importar en que parte se encuentre. El internet acorta los plazos de tiempo y proporciona una variedad de acceso a información (Ramón, 2016).

Según Anchundia (2017) las instituciones educativas han implementado las tecnologías de la información y la comunicación para mejorar los métodos de enseñanza y el desempeño de los estudiantes, aunque esta herramienta aporta beneficios también tiene desventajas ya que están expuestas ataques cibernéticos. El sector educativo ocupa el tercer lugar a nivel mundial en recibir ataques cibernéticos, en los puestos primeros están el sector financiero y seguido el gubernamental. Los cibercriminales les parecen más fácil atacar a las universidades puesto que algunas no cuentan con mediadas de protección adecuadas para proteger la información y la infraestructura de la

institución. Los cibercriminales buscan suplantar identidades, robar datos personales de estudiantes, de docentes y de trabajadores. Así mismo distribuyen malware maliciosos, realizan cambios no autorizados, alteran calificaciones, destruyen bases de datos, entre otras. Sin duda las universidades se han convertido en un el punto clave de ataques cibernéticos porque no solo tienen atacantes externos sino también poseen atacantes internos como los estudiantes curiosos que están aprendiendo estas herramientas tecnológicas y tratando de aplicar ese conocimiento y vulnerar la red de la universidad.

Yanes (2018) afirma que las universidades son entornos que están muy conectados al internet, cada día miles de alumnos y trabajadores usan computadores, portátiles, tablets y teléfonos inteligentes para acceder a la información de la institución además utilizan redes wifi que en ocasiones no son seguras, todos estos hechos atraen a los cibercriminales. En un informe que realizo la compañía Kaspersky (2018) indica que en el año 2017 se detectó 961 ataques de pishimg a 131 universidades en dieciséis países como Estados Unidos, Reino Unido, Australia, Canadá Finlandia, Hong Kong, India, Israel, Países Bajos, Nueva Zelanda, Polonia, Sudáfrica, Suecia, Suiza, los Emiratos Árabes Unidos y Colombia. Uno de los principales objetivos de los atacantes es conocer las contraseñas de los correos eléctricos institucionales, así como las direcciones IP y datos de ubicación de la institución educativa.

Gros (2015) dice que para tener esta información los cibercriminales diseñan páginas web parecidas a las de las universidades para que las victimas ingrese los datos de inicio de sesión y contraseña. Con estos ataques los cibercriminales tienen acceso a información general como nombres, número de identificación, correos electrónicos de los estudiantes y trabajadores de la institución educativa e incluso pueden saber sobre el salario de un empleado y la jornada laboral para más adelante desarrollar ataques precisos. El ciberespacio genera una serie de amenazas para

las instituciones educativas, por un lado, están los ataques cibernéticos que afecta la confidencialidad, la integridad, la disponibilidad de los sistemas informáticos de las universidades, por otro lado, los inconvenientes que se provoca por la carga informativa a la que se expone los estudiantes con la búsqueda de información en internet. Todo esto con lleva que los cibercriminales se aprovechen de estas situaciones, esto causa las siguientes amenazas:

2.2.1. Robo de Identidad. Debido al auge de las tecnologías de la información y la comunicación las universidades han tenido que enfrentar el problema del robo de identidad. Es uno de los principales métodos que utiliza lo cibercriminales para adquirir información de las víctimas (Sánchez, 2011).

2.2.2. Acoso, Chantaje y Extorsión. González (2014) señala que el robo de identidad en el ciberespacio provoca otro tipo de riesgo como el acoso, el chantaje y la extorsión. Los cibercriminales usan la información confidencial de los estudiantes y trabajadores de la universidad para acosarlos.

2.2.3. Filtros de Conexión. La ausencia de filtros de conexión en las universidades provoca que terceros puedan atacar la red y el sistema de la institución educativa. Los filtros de conexión ayudan impedir el acceso de información no autorizada (Brunner, Tedesco & Aylwin, 2003).

2.2.4. Servicios de la Nube. Tünnermannos (2003) manifiesta que los servicios de nube son programas que se alojan en uno o varios servidores ubicados físicamente en cualquier parte del mundo. Aunque estos servicios tienen mecanismos de seguridad, es fundamental que las universidades protejan la privacidad de la nube con la finalidad de evitar que los cibercriminales se aprovechen de la más mínima vulnerabilidad. Si la institución educativa no cuenta con un sistema ciberseguridad pueden obtener información de contenidos educativos o mecanismos de evaluación, entre otros datos.

2.2.5. Intranets. Los intranets son mecanismos que permite compartir información a los usuarios. Si las universidades no poseen un sistema de ciberseguridad puede colocar en peligro la información sensible almacenada en las intranets como por ejemplo investigaciones y proyectos académicos que es uno de los activos más apreciados por las instituciones educativas (Gros, 2015).

2.2.6. Búsqueda de Información. Sánchez (2011) indica que el exceso de información que se ha generado por el internet y la búsqueda de datos que hace diferentes estudiantes han permitido que cibercriminales se aproveche de esta vulnerabilidad para distorsionar y falsificar la información de las páginas web de las instituciones educativas.

**2.3**. Informes de Ataques Cibernéticos en las Universidades de Colombia

Según Yohai (2019) los ataques cibernéticos en las universidades en Colombia reflejan un crecimiento gradual pues la Policía Nacional en el año 2019 registro 10.000 casos, del total de los casos registrados 5.000 fueron denunciados como infracciones a la Ley 1273 de 2009. En comparación al año 2018 las denuncias informáticas aumentaron en el 2019 un 10%. Los ataques más reportados por los estudiantes y directivos de los centros educativos es el phishing con un 50%, la suplantación de identidad un 20%, el envío de malware un 17% y los fraudes de pago en línea un13%. La motivación principal de los cibercriminales es obtener la mayor información posible para tener una ventaja económica sobre las víctimas. Los delitos informáticos más denunciados por las universidades en Colombia son: el hurto, los cibercriminales conocen que el dinero está en las cuentas bancarias por esta razón buscan comprometer los sistemas de la institución educativa para interactuar con la entidad bancaria, el segundo lugar, está la violación de datos personales, para obtener esta información los cibercriminales suplanta la personalidad de la víctima, el tercer delito es el acceso abusivo a sistema informático, en el cuarto lugar se encuentra la transferencia no consentida de activos y el quinto delito es el uso de software

malicioso. Las universidades que más sufre ataques cibernéticos son las que están ubicadas en Bogotá, Honda Tolima, Cartagena, Antioquia y Amazonas.

El 90% de los ataques cibernéticos en las universidades de Colombia se deben a ingeniería social, por medio de técnicas puede tener información confidencial de los estudiantes, directivos y trabajadores de la institución educativa para después suplantar la identidad con la finalidad de que realicen acciones no autorizadas que conllevan a defraudar a la institución para luego desviar dinero hacia cuentas bancarias. Para poder retirar el dinero, los ciber atacantes abren cuentas bancarias con datos y documentación sustraída de las universidades y dispersan el dinero por medio mulas bancarias que son personas que prestan las cuentas bancarias para recibir dinero producto de actividades ilícitas. Las principales fuentes de engaño son: correos fraudulentos (spear phishing), enmascaramiento de correos (spoofing) e infección de sitios frecuentemente visitados por estudiantes y empleados de la universidad (Yohai, 2019).

**2.4**. Tipos de Ataques Cibernéticos más Comunes en las Universidades

Kaspersky (2018) afirman que los tipos de ataques cibernéticos más comunes en las universidades son:

2.4.1. Ransomware. Según Kaspersky (2016) el ransomware se puede definir como ciber secuestro de datos. Consiste que un software malicioso infecta el equipo y encripta a los archivos obligando a la víctima a realizar un pago para recuperar la información. Este tipo de malware se camufla dentro de otro archivo apetecible para que el usuario haga clic, por ejemplo, puede ocultarse en los archivos adjuntos como en Gmail, videos de páginas web de dudoso origen e incluso en programas o actualizaciones de sistemas. Una vez que ha penetrado en el ordenador el malware se activa y provoca el bloqueo del todo el equipo y encripta la información. Una de las particularidades sobre este ataque es que los cibercriminales envían un mensaje de advertencia con

la amenaza y el importe que tiene que pagar para recuperar la información. Este se suele enviar mediante correo electrónico, páginas web, llamada, transferencia o SMS. Para potenciar la incertidumbre y el miedo de la víctima en ocasiones incluye la dirección IP, la compañía proveedora de internet e incluso una fotografía tomada de la webcam. En muchos casos, aunque pague la víctima no le regresa la información y como única opción le queda formatear el equipo.

Yépez, Alvarado, Ortiz & Acosta (2017) afirman que existen dos tipos de bloqueo sin encriptación y con encriptación, el primer tipo de bloqueo es una toma del sistema sin encriptar datos, este malware desactiva el administrador de tareas e infecta el fichero Explorer.EXE esto hará que desparezcan los iconos de escritorio e impedirá que se usen los programas, por otra parte, también está el bloqueo con encriptación que encripta los datos del disco duro con códigos casi imposibles de descifrar y la encriptación solo afecta archivos del sistema. Un antivirus podrá recuperar la información reinstalándolo, pero si esta encriptada todo el sistema operativo o lo que es peor los datos del usuario habría que formatear el disco duro con la inevitable perdida de datos. Los ataques de ransomware no son nada nuevos llevan décadas usándose, se ha incrementado en los últimos años. Si una universidad se ve afectada por ransomware puede llegar a bloquear la operatividad del sistema esto afectaría el funcionamiento de la institución educativa.

2.4.2. Spyware. Boldt, Carlsson & Jacobsson (2010) sostienen que el spyware es un software malicioso especial que recopila información de un dispositivo y después transmite esa información a una entidad externa sin el consentimiento o sin la autorización del propietario y posee la particularidad de poder instalarse en cualquier sistema operativo de forma furtiva, es decir, sin que el usuario pueda darse de cuenta de que el equipo se instaló el spyware. Uno de los efectos que provoca los spyware es la lentitud de los sistemas operativos, en la ejecución del programa se bloquean o se apagan porque consumen recursos de los equipos impidiendo que funcione

normalmente. El spyware infecta el sistema operativo disminuyendo el rendimiento del equipo. Tiene como objetivo puntual capturar y monitorizar los movimientos del equipo de las víctimas

2.4.3. Keyloggers. Dadkhah, Ciobotaru, Davarpanah & Barati (2014) manifiestan que un keyloggers es un software que tiene como función registrar todo lo que se pulse en el teclado de la computadora. Este tipo de programas guardan la información de los sitios de internet que visita la víctima sin importa a que página entre ya sea Facebook, Twitter, Messeguer o YouTube el keyloggers siempre va registrar todo lo que escriba la víctima.

2.4.4. Phishing. Sastoque & Botero (2015) definen el phishing como una técnica que utiliza los cibercriminales para suplantar la identidad de una persona o institución para obtener datos confidenciales de las víctimas como nombres, direcciones, fechas de nacimiento, contactos personales, información salarial y cuentas de bancos, así como los registros académicos de estudiantes. Para posteriormente utilizar esos datos en beneficio propio. Los medios que usa para hacer este ataque son el correo electrónico, el SMS, las llamadas telefónicas e incluso hacen páginas web parecidas a la organización para que las víctimas no desconfíen y accedan al sistema.

2.4.5. Intervención de las Redes Sociales. Los cibercriminales analizan las redes de las instituciones educativas para encontrar alguna vulnerabilidad en la seguridad, de esta forma envía un comando al servidor que causa que la red se bloquee para después ejecutar el código, al acceder a la red se puede obtener toda la información que este almacenada. Esto provoca un gran daño al punto que los demás equipos se pueden bloquear (Sánchez, 2011).

2.4.6. Spoofing. Echaiz & Ardenghi (2015) establecen que el spoofing se puede traducir como engañar, en términos de seguridad informática se refiere al uso de técnicas de suplantación de identidad, suele estar relacionados con malware maliciosos o de investigación. Según Muñoz, Salazar & Yang (2016) existe distintos tipos de spoofing entre ellos tenemos:

*2.4.6.1. IP Spoofing.* El IP spoofing consiste en sustituir la dirección IP origen de un paquete TCP-IP por otra IP que desea suplantar. Esto se consigue a través de programas así las respuestas del host que reciba los paquetes alterados irán dirigidas a la IP falsificada.

*2.4.6.2. ARP Spoofing.* El ARP spoofing se encarga de suplantar las tramas ARP de esta forma consigue enviar los equipos atacados a un host en el que los datos del equipo están en las manos de un cibercriminal. Para llevar a cabo el objetivo el atacante consigue duplicar las tablas que contiene las tramas ACR esto permite forzar a enviar paquetes a un host controlado por el atacante.

*2.4.6.3. DNS Spoofing.* El DNS spoofing consiste en falsificar un IP para que mediante un nombre de DNS consiga una IP. Para conseguirla puede comprometer al servidor que infecta la cache de otro o modificando las entradas del servidor.

*2.4.6.4. Web Spoofing.* Consiste en suplantar una página web real por una falsa, para conseguir datos de los usuarios. La página falsa actúa de modo de proxy y se solicita información pedida por la victima a cada servidor original llegando a evitar la protección SSL.

*2.4.6.5. Email Spoofing.* El email Spoofing consiste en suplantar una dirección de correo electrónico. Esta técnica se usa con asiduidad para él envió de correos hoax como suplemento perfecto para el uso de phising y spam

**2.5**. Casos de Ataques Cibernéticos documentados de Universidades en Colombia.

A continuación, se citan algunos casos de ataques cibernéticos que ha sufrido las diferentes universidades en Colombia:

2.5.1. Universidad de los Andes. La Universidad de los Andes sufrió los siguientes ciberataques:

- Donoso (2018) indica que en el año 2013 el estudiante de ingeniería civil Alejandro Robayo a causa de las bajas calificaciones que había obtenido en el primer semestre de ese año, decidió aplicar los conocimientos en sistemas para modificar las notas y no perder la beca que había obtenido. El estudiante de ingeniería (insider) pasó de implementar los conocimientos de informática de manera personal, para luego utilizarlo con fines lucrativos entre los demás compañeros de la universidad. Después empezó a crear un correo electrónico clandestino en el que diversos estudiantes pudieran contactar los servicios para modificar las calificaciones de los parciales por el valor de setenta y cinco mil a noventa mil pesos. Aunque los servicios prestados por Robayo eran de forma anónima, fue descubierto por una estudiante que le parecía injusto que algunos estudiantes obtuvieran buenas calificaciones a causa de este tipo de ventajas informáticas, decidió notificar a la universidad sobre esta problemática.

  Las directivas de la institución al enterarse de dicha situación procedieron de inmediato a iniciar un proceso disciplinario en contra del estudiante y la expulsión del mismo, que conlleva consigo al impedimento de que el estudiante sancionado no se pueda graduar en dicha institución. En febrero del año 2015 Alejandro Robayo fue condenado por las autoridades judiciales por los delitos de acceso abusivo a sistema informático y uso de software malicioso. Según la información suministrada por la fiscalía general de la Nación el implicado pudo realizar este tipo de actuaciones por medio de la utilización de keyloggers la cual, le permitió identificar los correos electrónicos institucionales y contraseñas de los profesores de la universidad. Aunque fue condenado a tres años de cárcel la administración de justicia decidió beneficiarlo con la pena no privativa de la libertad

debido que era el primer delito y no tenía un gran historial criminal que determine la detención carcelaria (Donoso, 2018).

- Porras (2018) señala que el 7 de marzo del 2016 fueron hackeadas la página web de la institución que permitía consultar toda la información de la nueva maestría en propiedad intelectual. El ataque cibernético paralizo la página de la universidad durante una hora y media. Aunque no se tiene certeza de quien realizo el ciberataque se cree que el grupo de hackers autodenominados Anonymous fue quien perpetro el ciberataque. Las autoridades afirman que el ataque se debe a ideales hacktivistas que ven a dicha maestría como una limitación a la libertad de expresión e información de los cibernautas.

2.5.2. Universidad de Cartagena. El 20 de febrero de 2015 las autoridades judiciales condenaron a Richard Gonzales Cohen a una condena de 12 años y 5 meses de cárcel por fraude electrónico que realizo en marzo del año 2009 con la finalidad de hurtar más de 3.000 millones de pesos de las cuentas bancarias que tenía la institución educativa en el Banco GNB Sudamerin. Según las investigaciones hechas por la administración de justicia el dinero hurtado fue consignado a cuentas de diferentes personas dentro de las cuales hacen parte de las cuentas bancarias del extesorero de la universidad y 23 personas más que aportaron cuentas bancarias para la realización de la transacción bancaria. En la audiencia realizada fueron escuchados los testimonios del rector de la universidad señor German Sierra Anaya para esclarecer los hechos ocurridos y conocer de una forma detallada como se realizó la millonaria estafa electrónica a las cuentas de la universidad (Cano, 2016).

2.5.3. Universidad de Amazonas. Esplandiu (2017) señala que los estudiantes en ingeniera alimenticia Ana Yesenia Silva Cuellar y Sandra Milena Peña Gonzales en el año 2015 con los conocimientos en computación lograron ingresar a los sistemas informáticos de la universidad con

la finalidad de obtener el título profesional de forma más rápida alterando los datos de los sistemas de la institución. Las dos estudiantes lograron el cometido y recibieron los diplomas en ese mismo año. Meses después de que se hubieran graduado, se logró descubrir por medio de la revisión realizada por la auditoria de la universidad que las bases de datos tenían una serie de modificaciones en lo que respecta al cumplimiento del pensum, las cargas académicas y los requisitos de grado, por esta razón, la rectoría de la institución puso en conocimiento a las autoridades sobre el ataque cibernético.

Las investigaciones realizadas se descubrieron que las procesadas ingresaron de manera no autorizada a los sistemas de la universidad por medio, de un gestor de datos sin que fuera necesario utilizar las aplicaciones informáticas de la universidad, logrando que el sistema creyera que ya habían cumplido con todos los requisitos para graduarse. Sin embargo, las copias de seguridad delataron la intromisión. Las dos estudiantes fueron culpadas por los delitos de fraude procesal y daño informático, debido que las partes implicadas llegaron a un acuerdo con la justicia y confesaron la realización de las conductas, el juzgado les beneficio con la suspensión de la pena privativa de la libertad y él deber de indemnizar por los daños causados a la institución educativa (Esplandiu, 2017).

2.5.4. Universidad del Tolima. Según Betancourt, Monroy & Dávila (2015) la realización del ataque fue informada por parte de la Oficina de Gestión Tecnológica de la Universidad del Tolima en enero del año 2018 también informaron a los cargos administrativos y a la rectoría de la instrucción, sobre ciertas inconsistencias en las notas de más de 18.000 estudiantes que habían cursado el segundo semestre académico de finales de año del 2017, las notas académicas de gran parte de los estudiantes habían sido modificadas para que quedaran con la nota más alta. La rectoría junto con los expertos en ciberseguridad de la institución informó que los ataques no habían podido

ser ejecutados por un estudiante sino más bien por un hacker que realizo cada una de las operaciones. Aunque se desconocen los motivos por los cuales se propiciaron dichos ataques, la universidad interpuso ante la fiscalía general de la Nación una denuncia por acceso abusivo a sistemas informáticos.

Las autoridades han planteado dentro de las investigaciones la magnitud y el conocimiento de la intromisión realizada, lo más posible es que este tipo de ataques fueron ejecutados por alguien (Insider) que conocía las bases de datos que almacenaban las notas de los estudiantes y la estructura interna de los sistemas de la universidad. Los ataques realizados conllevaron a la institución a suspender el acceso de las plataformas digitales hasta poder restablecer todas las notas del segundo semestre académico de 2017. Debido a los incidentes la Universidad del Tolima ha tomado la decisión de mejorar las medidas de seguridad de los sistemas y las bases de datos con el fin de evitar que este tipo de problemáticas no vuelvan a suceder (Betancourt et at., 2015).

2.5.5. Universidad Distrital Francisco José de Caldas. León & Bonilla (2017) establecen que el 10 de diciembre de 2018 las bases de datos de la Universidad Distrital Francisco José de Caldas fueron hackeadas por cibercriminales con el propósito de conocer datos personales e información financiera de la universidad. Para obtener estos datos los cibercriminales enviaron un correo electrónico malicioso (phishing) a la universidad para apoderarse de la cuenta del correo de los empleados de la institución y de esta manera generar comunicados y correos falsos a los empleados responsables de realizar los pagos o transferencias. Con base a esta información los ciber atacantes pueden engañar a los estudiantes de la universidad para que hagan los pagos de matrícula a las cuentas que tienen bajo control los cibercriminales.

2.5.6. Universidad de Antioquia. Lopera (2020) manifiesta que el 16 de abril del 2020 la aplicación Zoom fue hackeada en plena conferencia virtual que trataba sobre los factores

psicosociales del teletrabajo. Los 170 los estudiantes de la Universidad de Antioquia se encontraban tranquilamente viendo la conferencia cuando de repente una imagen muy asustadora se apodero de la pantalla interrumpiendo la videoconferencia. La universidad ofreció desde la cuenta oficial disculpas por las fallas técnicas generadas por el hackeo presenciado. Aunque todavía no se sabe quién realizo el hackeo. Los expertos de ciberseguridad de la unidad virtual de la institución informaron que un grupo de ciberdelincuentes se habían infiltrado en las sesiones de la plataforma Zoom para impedir la realización de la videoconferencia. Zoom es una de las plataformas digitales más utilizadas por la gran mayoría de universidades del país para realizar clases virtuales.

Desafortunadamente la Universidad de Antioquia al igual que muchas instituciones que han decidido utilizar la aplicación, han padecido las fallas técnicas y ataques cibernéticos. Estas intromisiones son utilizadas por los hackers para vulnerar la seguridad de las plataformas. Los dueños de la plataforma Zoom han informado que buscan la asesoría de compañías expertas en seguridad informática para que los mismo busquen las fallas en el sistema que permitan que intrusos ingresen a la aplicación de forma no autorizada y las puedan solucionar con la utilización de filtros de seguridad en los cuales solo pueden ingresar las personas que hagan parte de la institución (Lopera, 2020).

2.5.7 Universidad de El Bosque: La universidad del bosque sufrió un ataque cibernético por parte de hackers el día 28 de junio de 2021 en horas de la madrugada. Estos delincuentes cibernéticos se apoderaron de todas las cuentas de correo electrónico de la universidad e incluso de la cuenta de la universidad alojada en la red social Twitter según informes dados por ese medio. La universidad sacó un comunicado solicitando a sus estudiantes y trabajadores que desvincularan las cuentas de sus teléfonos, computadores y en todo sitio en el cual se encontrara vinculada su

cuenta ya que sus datos podrían ser robados ya que toda la información podría estar comprometida. “La universidad ha sido víctima de un ciberataque de seguridad, por el cual algunos de nuestros sistemas internos han sido comprometidos", citado por la entidad en su comunicado. El Bosque aseguró que "actualmente, el personal especializado y las directivas de la universidad están trabajando activamente en la atención de la situación y, al mismo tiempo, se está implementando el plan de acción para solucionar el evento en el menor tiempo posible y garantizar la continuidad de la operación". (El Tiempo, Julio 28 2021). Mediante la cuenta de Twitter de la Universidad de El Bosque los ciberdelincuentes preguntaron que cuál universidad les gustaría que fuera atacada. Cabe resaltar que los estudiantes se tomaron el ataque como algo divertido y lo volvieron tendencia en grupos de Facebook y en Twitter.

Finalmente, en términos generales, Según KASPERSKY (2020) Es interesante observar que la cantidad de ataques DDoS a recursos web educativos y administrativos se ha triplicado en comparación con el mismo período en 2019. Además, tales ataques en el primer trimestre de 2020 representaron el 19% del número total de incidentes, mientras que hace un año solo representaban el 11%.

El aumento del interés de los ciberdelincuentes en dichos recursos puede estar asociado con la propagación de la infección por COVID 19, lo que ha hecho que los servicios de educación a distancia y las fuentes oficiales de información sean más populares. Desde principios de 2020, la epidemia ha afectado a todos los sectores, ya que la mayoría de las actividades productivas, educativas y de entretenimiento se han traslado al ciberespacio, es decir se ha aumentado la superficie expuesta a los ataques.

# 3. CAPITULO III

## 3.1. Metodologías que Analizan el Costo y Beneficio de las Inversiones en Ciberseguridad

Las redes sofisticadas, los sistemas altamente conectados en la red y el creciente valor de la información almacenada en internet permite que el acceso a la información sea distribuido globalmente a un número incontable de personas. Esto hace que las organizaciones sean más vulnerables a los ataques cibernéticos. Los cibercriminales tienen por objeto robar o suplantar identidades, el espionaje y la interrupción de las operaciones de infraestructura crítica. Los ciberataques más comunes son la denegación de servicios, el malware, el virus, los gusanos o troyanos, los ataques basados en web y el phishing (Niño, 2015).

Según Villa (2018) los ataques cibernéticos no solo causan pérdidas económicas sino también afecta la marca, el buen nombre y la reputación de la compañía. Por esta razón la organización tiene que analizar las inversiones en ciberseguridad para minimizar las pérdidas que provoca las amenazas cibernéticas. La cantidad invertida en seguridad debe basarse en un análisis de costo y beneficio para evaluar los riesgos y la efectividad de la medida de ciberseguridad.

Montealegre (2018) afirma que el análisis de costo y beneficio es una herramienta que le permite a las organizaciones a corto, mediano y largo plazo enfrentar de forma eficiente los retos propuestos por los constantes y complejos cambios políticos, sociales, y tecnológicos que se presenta en el desarrollo de la sociedad, además analiza las inversiones en ciberseguridad para de esta manera tomar decisiones adecuadas que ayude reducir las amenazas y optimiza los recursos de la empresa.

Bistarelli, Fioravanti & Peretti (2006) señalan que las metodologías que analizan el costo y beneficio de las inversiones en ciberseguridad son el análisis cuantitativo y el análisis cualitativo. A través de estos dos métodos la organización puede identificar el riesgo, cuantificar el daño, calcular la probabilidad de ocurra y medir la perdida en caso que suceda la amenaza e incluso puede determinar los costos de prevención del riesgo. Para conocer más de estas metodologías a continuación se explica cada una:

## 3.2. Análisis Cuantitativo

En este apartado se trata la definición, los índices que usa la metodología cuantitativa para calcular el costo y beneficio de la inversión en ciberseguridad, el proceso del análisis cuantitativo, por último, se desarrolla un ejercicio práctico la cual se indica los pasos para hacer este tipo de análisis.

### 3.2.1. Definición de Análisis Cuantitativo.

A continuación, se citan algunos autores que definen el análisis cuantitativo:

Caballero (2013) señala que el análisis cuantitativo es un método objetivo que evalúa la probabilidad, el impacto y analiza escenarios de alcance, tiempo y costo de un determinado riesgo.

Holtsnider & Jaffe (2012) afirman que el análisis cuantitativo es un método que utiliza las organizaciones para analizar los efectos que provoca los ataques cibernéticos. Por medio de esta metodología se puede calcular la cantidad del daño, la probabilidad de que ocurra y la pérdida probable en caso que se presente el riesgo.

Rosenquist (2008) define el análisis cuantitativo como una evaluación que fija valores monetarios a los activos de la compañía, a los daños y a las pérdidas que causa los riesgos cibernéticos, a las amenazas, a las vulnerabilidades, a los impactos, a la frecuencia de las amenazas y a las

salvaguardias para determinar el costo del riesgo para después implementar una estrategia de mitigación contra los ciberataques.

De acuerdo a las definiciones anteriores todos los autores concuerdan que el análisis cuantitativo es una metodología que se usa para calcular la probabilidad, el impacto, la frecuencia y perdida que causa una amenaza cibernética a un determinado activo. Mediante este método se puede diseñar medidas de ciberseguridad más eficaces y acorde a la capacidad económica de la organización.

3.2.2. Índices del Análisis Cuantitativo. Según Bistarelli et al. (2006) el análisis cuantitativo usa los siguientes índices para calcular el costo y beneficio de la inversión en ciberseguridad:

*3.2.2.1.* Valor del activo. Moncayo (2014) dice que el valor del activo es conocido por las siglas en inglés AV es el valor monetario asignado a un activo basado en el costo de mantenimiento, soporte, reparación y reemplazo. El valor del activo hace referencia ¿Cuánto le costó este activo a la organización? y ¿Cuánto dinero perderá la organización si este activo falla o se repara o si es atacado por un ataque cibernético?

*3.2.2.2.* Factor de exposición. Hathaway (2018) manifiesta que el factor de exposición es representado por las siglas en inglés (EF) es el porcentaje del activo perdido por un ataque. El factor de exposición representa el impacto del riesgo sobre el activo, o porcentaje de activo perdido. Por ejemplo, si el valor que está en riesgo es de dos tercios el valor del activo, esto quiere decir que el factor de exposición es 0.66. Si el activo se pierde el factor de exposición es de 1.0.

3.2.2.3. Expectativa de pérdida única. Según Kumar, Ali & Fatema (2014) la expectativa de pérdida única es reconocida por la sigla en inglés (SLE) se refiere a la pérdida monetaria cada vez que un activo de la organización está en riesgo. El SLE es un valor monetario que describe

cuánto costará el incidente a la organización, en otras palabras, es el IMPACTO de un ataque. Es un término que se usa con más frecuencia durante la evaluación de riesgos e intenta asignar un valor monetario a cada amenaza. Se calcula SLE de la siguiente manera:

$$SLE = Valor\ del\ activo\ (AV) x\ Factor\ de\ exposición\ (EF)$$

Donde el valor del activo (AV) es el costo de creación, desarrollo, soporte, reemplazo y valores de propiedad del activo y el factor de exposición (EF), está una representación del dolor causado a la víctima, se representa como una función de normalización de la curva del dolor entre 0 y 1. Donde 0 significa que el ataque no causa ningún impacto en el activo y 1 representa que el ataque causó un daño catastrófico equivalente al 100% al valor del activo objeto del ataque. En otras palabras (EF) estima la pérdida o el impacto en el valor de un activo cuando surge un riesgo o una amenaza y se representa como un porcentaje del valor del activo. Por ejemplo, si un activo está valorado en $100.000 dólares y el factor de exposición del activo es del 25%, la expectativa de pérdida única es de $25.000 dólares ($100.000 x 25% = $ 25.000) (Dzarma, Abdulkadi & Idama, 2015).

Gregg (2007) indica que la expectativa de pérdida única del valor del activo (AV) y el factor de exposición (EF) permite ajustar dos términos de forma independiente: el valor del activo puede variar con la inflación, los cambios del mercado, etc., mientras que la introducción de medidas preventivas reduce el factor de exposición.

*3.2.2.4. Tasa de ocurrencia anualizada.* Bella, Bistarelli, Peretti & Riccobenea (2007) establecen que la tasa de ocurrencia anualizada es conocida por la sigla en inglés (ARO) determina con qué frecuencia puede ocurrir el ataque cibernético en un año. Es fundamental conocer esta información para dimensionar el impacto de la amenaza durante ese periodo de tiempo. Esto corresponde a una variable de entrada al modelo.

*3.2.2.5. Expectativa de pérdida anualizada.* Vivanco, Cortez & Bustamante (2011) afirman que la expectativa de pérdida anualizada es representada por la sigla en inglés (ALE) es la cifra de dinero que se podría perder una organización en un año por causa de un riesgo o amenaza cibernética. El ALE identifica el monto de presupuesto anual máximo para gastar en la protección de un activo, el costo de implementar medidas de ciberseguridad cada año no debe exceder el ALE. Para calcular el ALE se usa la siguiente fórmula:

$$ALE = Expectativa\ de\ perdida\ única\ (SLE) x\ Tasa\ anualizada\ de\ ocurrencia\ (ARO)$$

Donde la expectativa de pérdida única (SLE) representa la pérdida potencial por la materialización de una amenaza, y la tasa anualizada de ocurrencia (ARO) es la cantidad de veces que un riesgo o evento puede ocurrir en un año. Se calcula multiplicando la expectativa de pérdida única (SLE) y la tasa anualizada de ocurrencia (ARO) (Bistarelli et al., 2006).

Según Osborne (2006) el cálculo del ALE permite a las empresas planificar pérdidas potenciales e implementar estrategias adecuadas para poder enfrentar los riesgos que provoca los ataques cibernéticos. Si el valor del ALE supera el costo del activo, la inversión en ciberseguridad es viable para la organización, pero si el costo de las medidas de ciberseguridad supera el valor del activo, la implementación de la medida de protección no resulta rentable para la compañía.

Por ejemplo, si la pérdida de expectativa anualizada (ALE) por una amenaza que ocurre es de $ 4.000 de dólares y el costo de las acciones para evitar el riesgo es de $ 6.000 de dólares sería más económico para la empresa no realizar actividades para reducir la pérdida esperada. Por el contrario, cuando el análisis muestra que el beneficio supera la pérdida esperada, se podría tomar medidas para evitar la amenaza (Conrad, Misenar & Feldman, 2014).

Cole (2013) establece que el ALE tiene ventajas para medir y evaluar la pérdida, pero también presenta ciertos inconvenientes pues estas medidas se expresan en valor monetario, por tanto, algunos valores asignados a un riesgo pueden estar sujetos a la opinión personal o basarse en la experiencia o intuición. Aunque el ALE tiene algunos inconvenientes, las organizaciones lo utilizan porque es fácil de comprender los resultados.

*3.2.2.6. Retorno de la inversión.* Sánchez (2018) dice que el retorno de la inversión es conocido por las siglas en inglés (ROI) es un índice financiero que se utiliza para calcular el beneficio que recibirá una organización en relación con una determinada inversión. Cuanto mayor sea la proporción, mayor será el beneficio obtenido. La ecuación del ROI es:

ROI = Beneficios / Inversión.

Beneficios = Ingresos – Costos; asociados al proyecto de inversión.

Es un indicador de rentabilidad de la inversión. Los beneficios son la utilidad producida por una inversión realizada. Es decir, cuánto dinero se gana por la inversión hecha.

Para el responsable de ciberseguridad de una Entidad Pública o Privada, le queda muy difícil demostrar cuales son los beneficios económicos tangibles, por lo tanto, NO es posible calcular el ROI de dicha inversión, tal como está escrito en los libros de finanzas. Lo que sí se puede calcular son las posibles pérdidas en que incurriría la organización si dicha inversión no se hace. En otras palabras, lo que sí se puede calcular es la expectativa anual de perdida (ALE) y el riesgo residual (riesgo remanente) que persiste después que una organización ha realizado dicha inversión en una contramedida. Esto da origen al concepto de ROSI (Retorno de la inversión en sistemas de seguridad). Según Sonnenreich (2005), define el ROSI así:

$$ROSI = \frac{((ALE\ X\ RM) - CSI)}{CSI}$$

Donde (ALE) es la expectativa de pérdida anualizada, (RM) es el riesgo mitigado por una medida de protección que mitiga el riesgo de pérdida derivado de la explotación de una vulnerabilidad y (CSI) es el costo de inversión en seguridad que una organización debe invertir para implementar la medida de ciberseguridad. Si el ROSI arroja un número superior a cero la inversión es favorable, pero si es un número inferior a cero la inversión no es viable (Bistarelli et al., 2006).

Según Ángulo (2020) para calcular el ROSI de la seguridad cibernética implica primero calcular el valor de las posibles pérdidas anuales así: el costo promedio de un incidente y multiplicar ese número por cuántos incidentes podría experimentar una empresa en un período de tiempo determinado. Con una aproximación de las pérdidas anuales derivadas de un respectivo ataque, las empresas pueden evaluar si la inversión en ciberseguridad es rentable.

*3.2.2.7. Retorno del ataque.* Según Bistarelli et al. (2006) el retorno del ataque es representado por la sigla en inglés (ROA) es la ganancia que un atacante obtiene por un ataque cibernético sobre las pérdidas que sufre por la adopción de la medida de protección que es la parte del objetivo del atacante. Para calcular el ROA se usa la siguiente fórmula:

$$ROA = \frac{GI}{Costo\ del\ ataque\ antes\ de\ contramedidas + sobrecosto\ resultante\ de\ las\ contramedidas}$$

Donde (GI) es la ganancia que tiene un atacante sobre un ciberataque éxito y (Costo del ataque antes de que el defensor implemente las contramedidas + el sobre costo al que tiene que verse sometido el atacante como resultado de las contramedidas implementadas por el defensor). El ROA permite ejecutar una evaluación más completa de una mediada ciberseguridad pues no solo analiza la efectividad y la rentabilidad para el defensor sino también el efecto que produce sobre el atacante, entre menor sea el ROA, menor es el incentivo para realizar el ataque. (Bistarelli et al., 2006).

*3.2.2.8. Brecha de Control.* Vargas & Zubieta (2017) señalan que la brecha de control es reconocida por la sigla en inglés (CG) es el porcentaje del valor del activo que una contramedida no puede proteger. La brecha de control identifica la efectividad de la contramedida o los controles de seguridad implementados para el activo.

*3.2.2.9. Riesgo residual.* Reyes & Porras (2020) afirman que el riesgo residual conocido por las siglas en inglés (RR) es un valor monetario que identifica el costo del activo que las contramedidas no protegen. Para calcular el RR se utiliza la siguiente fórmula:

RR = Valor del Activo (AV) x Brecha de Control (CG)

*3.2.2.10. Valor presente neto.* Guigui & Salas (2012) manifiestan que el valor presente neto es representado por las siglas en inglés (NPV) o (VAN) calcula el valor presente o costo de la inversión que generará en el futuro, pero se debe tener en cuenta que el valor del dinero cambia con el tiempo por la inflación, la fiscalidad o el riesgo de la organización Para calcular el VAN se usa la siguiente fórmula:

$$VA = \frac{D}{(1+i)} + \frac{D2}{(1+i)^2} + \ldots + \frac{Dn}{(1+i)^n}$$

Donde (D) representa el valor de flujo de caja, (i) es la tasa de interés que se espera obtener o la tasa de retorno de una inversión de riesgo y (n) es el número de periodos que se calcula la inversión. Para determinar que una inversión en ciberseguridad es viable se debe restar el valor neto de la inversión inicial. La fórmula del VAN de una inversión inicial I es:

VAN =VA-I

Puga (2019) señala que el propósito de analizar diferentes inversiones es para saber si una inversión genera un mayor o menor valor a la organización. A continuación, se realiza un ejercicio práctico que explica cómo se calcula el valor presente neto:

El valor actual neto de dos inversiones tiene una tasa de retorno del diez por ciento y una inversión inicial de diez mil euros y posee los siguientes flujos de caja (Ver tabla 1):

*Tabla 1 Flujos de caja*

| Miles de euros | 2010 | 2011 | 2012 | 2013 | 2014 | Total, Flujos de Caja |
|---|---|---|---|---|---|---|
| Inversión A | (10.000) | 5.000 | 10.000 | 15.000 | 20.000 | 40.000 |
| Inversión B | (10.000) | 10.000 | 15.000 | 10.000 | 15.000 | 40.000 |

*Fuente: Tabla tomada de Puga, M. (2019).*

Durante 4 años las inversiones A y B tienen los mismos flujos de caja, para determinar cuál de estas dos inversiones es más rentable se debe calcular el VAN como se observa en la tabla 2:

*Tabla 2 El VAN*

| Miles de euros | 2011 | 2012 | 2013 | 2014 | Total, VA | VAN |
|---|---|---|---|---|---|---|
| Inversión A | 4.545 | 8.264 | 11.270 | 13.660 | 37.740 | 27.740 |
| Inversión B | 9.091 | 12.397 | 7.513 | 10.245 | 39.246 | 29.246 |

*Fuente: Tabla tomada de Puga, M. (2019).*

Analizando la inversión inicial de A y B frente al valor actual durante un periodo de 4 años tenemos que la inversión más rentable es B.

Si el VAN es mayor a cero significa que la invasión es rentable o si el VAN es igual a cero se genera un punto de equilibrio en la cual no se obtiene perdidas ni ganancia, pero si el VAN es menor que cero la inversión no es buena pues genera pérdidas económicas (Puga, 2019).

El problema en esta aproximación es calcular la tasa de descuento (tasa de interés) a la cual se deben descontar los flujos de caja. Dicha tasa de descuento generalmente está asociado al costo promedio de Capital (Patrimonio + Deuda), donde el costo del patrimonio (Ke) depende del costo de oportunidad de los accionistas de la organización o de los responsables de tomar las decisiones de inversión. El cálculo del Ke se sale del alcance de este trabajo de investigación.

3.2.3. Proceso del Análisis Cuantitativo. Cabeza & Cabrita (2006) dicen que el proceso de análisis cuantitativo implica cuantificar o colocar un valor monetario a todos los elementos que posee una organización como los activos, el impacto y la frecuencia de las amenazas, la probabilidad de que ocurra el ataque cibernético y el costo de las salvaguardas o contramedidas

Gregg (2007) afirma que para hacer el análisis cuantitativo tradicional se debe seguir los siguientes pasos:

*3.2.3.1. Primer paso: Determinar el valor del activo.* El primer paso en el proceso de análisis cuantitativo es determinar el valor del activo (AV), Cabeza & Cabrita (2006) dicen que los activos comúnmente examinados son: el hardware, el software, los servicios y la documentación. Al examinar un activo se debe analizar las siguientes preguntas para poder asignar un valor al activo: ¿Cuánto cuesta adquirir el activo?, ¿Cuál es la perdida si el activo se ve comprometido por un ciberataque?, ¿Qué importancia tiene el activo para la organización? y ¿Cómo afectaría su pérdida a la organización?

Oosthuizen, Pretorius, Mouton & Malekeng (2019) manifiestan que otro elemento que se debe tener en cuenta al momento de asignar un valor al activo es el:

- Costo de productividad.
- Costo de reparación.
- Costo para reemplazar el activo.

La valoración de activos es una tarea onerosa que requiere mucha experiencia y trabajo para realizarse correctamente.

*3.2.3.2. Segundo paso: Identificar amenazas.* El segundo paso del análisis cuantitativo es identificar amenazas, por lo tanto, la compañía debe recopilar información de cuáles son los activos, datos, programas o software que requiere de protección también es fundamental consultar a los altos directivos, a los representantes de recursos humanos y el personal en general para conocer las vulnerabilidades del sistema. La amenaza junto con una vulnerabilidad puede provocar pérdidas a la empresa por esta razón es importante identificar los riesgos cibernéticos para evitar pérdidas (Gregg, 2007).

Según Oosthuizen et al. (2019) la amenaza es cualquier circunstancia o evento que tenga el potencial de impactar negativamente un activo por medio de acceso no autorizado, destrucción, divulgación o modificación. Los tipos de amenazas son:

- Error humano.
- Error de procedimientos de seguridad del sistema.
- Mal funcionamiento del equipo.
- Software malicioso.
- Interrupción de la infraestructura critica de la organización.
- Divulgación de datos personales y robo de identidad.

Bistarelli et al. (2006) señalan que las vulnerabilidades son fallas o debilidades en los sistemas o software o procedimientos de seguridad. Los impactos que provoca las vulnerabilidades son:

- Pérdida de reputación.
- Pérdida de oportunidad comercial.
- Perdidas de activos.

*3.2.3.3. Tercer paso: Determinar el factor de exposición (EF).* El tercer paso del análisis cuantitativo es determinar el valor de exposición para conocer cuál fue el porcentaje del activo perdido por el ataque cibernético. A través de este factor, la organización puede analizar que tanto fue afectado o expuesto el activo al ciberataque (Gregg, 2007). Este factor es determinado por un juicio de expertos.

*3.2.3.4. Cuarto paso: Calcular la expectativa de pérdida única (SLE).* El cuarto paso del análisis cuantitativo es calcular la expectativa de pérdida única (SLE) para examinar cuanto fue la perdida que provocó un ataque cibernético al activo de la organización (Cabeza & Cabrita, 2006).

*3.2.3.5. Quinto paso: Asignar un valor a la tasa de ocurrencia anualizada (ARO).* El cuarto paso del análisis cuantitativo es calcular el valor de la tasa de ocurrencia anualizada (ARO) para que la organización pueda determinar ¿Con qué frecuencia ocurre la amenaza cibernética en un periodo de un año? (Gregg, 2007).

*3.2.3.6. Sexto paso: Asignar un valor a la expectativa de pérdida anualizada (ALE).* El sexto paso del análisis cuantitativo es asignar un valor a la expectativa de pérdida anualizada (ALE) para calcular la pérdida de un riesgo durante un periodo de un año. A través del ALE la organización determina qué amenazas deben recibir la mayor atención (Bistarelli et al., 2006).

*3.2.3.7. Séptimo paso: Evaluar los datos.* El séptimo paso es evaluar los datos y decidir si la inversión que se va a realizar en ciberseguridad es rentable o no para la organización.

Según Oosthuizen et al. (2019) el proceso de análisis cuantitativo tiene por objeto identificar los riesgos, asignar costos a los activos, a la información, al software, a las amenazas y determina los impactos de los mismos para que, la organización puede implementar medidas ciberseguridad más efectivas.

3.2.4. Ejercicio Práctico del Proceso de Análisis Cuantitativo. A continuación, se realiza un ejercicio práctico para explicar cómo se realiza el proceso de análisis cuantitativo:

La organización ha instalado un nuevo servidor de correo electrónico valorado en $2.500 dólares y planea usarlo para conectar 65 computadores. Actualmente, este servidor no tiene software instalado para spam o filtrado de contenido tampoco tiene antivirus. Hay un 95% de posibilidades que el nuevo servidor de correo electrónico sea atacado por un ataque cibernético. Si se produjera un ataque podría estar expuesto a un 75% de perder tres cuartas partes de los datos e incluso la red puede caer durante cuatro horas y desviar al equipo de soporte de las funciones normales que realiza. La organización va desarrollar el siguiente análisis cuantitativo para determinar si los $175 dólares que es el costo del antivirus es una inversión rentable o no para la compañía (Gregg, 2007).

*3.2.4.1. Primer paso: Determinar el valor del activo.* En este caso el activo o el servidor de correo electrónico tiene un valor de $2.500 dólares.

*3.2.4.2. Segundo paso: Identificar amenazas.* Por falta de una medida de ciberseguridad el servidor de correo electrónico de la organización puede ser atacado por un ataque cibernético. Los efectos de este ataque es la perdida de tres cuartas partes de los datos, la red puede caer durante cuatro horas y desviar al equipo de soporte de las funciones que normalmente realiza.

*3.2.4.3. Tercer paso: Determinar el factor de exposición (EF).* El factor de explosión (EF) es de 75%. El factor de exposición identifica el porcentaje del valor del activo que se verá afectado por la ejecución exitosa de la amenaza.

*3.2.4.4. Cuarto paso: Calcular la expectativa de pérdida única (SLE).* El valor de SLE es una cifra en dólares que representa la pérdida del activo. Para calcular la expectativa de pérdida única en el presente caso se usa la siguiente ecuación:

SLE =Valor del Activo AV×Factor de Exposición (EF)

SLE= Valor del Activo es de $ 2,500 x Factor de Exposición es de 75%=$1.875.

*3.2.4.5. Quinto paso: Asignar un valor a la tasa de ocurrencia anualizada (ARO).* El ARO es un valor que representa la frecuencia estimada con la que se espera que ocurra una amenaza determinada. En pocas palabras, ¿Cuántas veces se espera que el riesgo suceda en un año? En este caso indica que existe una probabilidad del 95% que ocurra un ataque cibernético.

*3.2.4.6. Sexto paso: Asignar un valor a la expectativa de pérdida anualizada (ALE).* Para este caso el ALE se calcula de la siguiente manera:

ALE = Expectativa de Pérdida Única (SLE) x Tasa Anualizada de Ocurrencia (ARO)

ALE= $ 1.875 (SLE) x 0.95 (ARO) = $ 1.781.

*3.2.4.7. Séptimo Paso: Evaluar los datos.* En este caso como el valor del ALE$ es de $ 1.781 dólares, por lo tanto, supera el valor de la medida de ciberseguridad que es el antivirus $ 175 dólares, es una inversión rentable para la organización.

$ 1.781 (ALE) - $ 175 (antivirus) = $ 1. 606

## 3.3. **Análisis Cualitativo**

En este apartado se explica la definición, los tipos de análisis que usa la metodología cualitativa para calcular el costo y beneficio de la inversión en ciberseguridad y el proceso del análisis cualitativo.

3.3.1. Definición de Análisis Cualitativo. Ochoa (2019) define el análisis cualitativo como un procedimiento mediante en el cual busca reducir la incertidumbre enfocándose en los riesgos de alto y de menor ocurrencia en un determinado evento, este procedimiento tiene como objetivo realizar una evaluación para medir los factores de probabilidad, áreas de exposición al riesgo y el daño que pueden producir para establecer una valorización de los riesgos y categorizarlos de mayor y menor amenaza.

Según Holtsnider & Jaffe (2012) el análisis cualitativo es un método subjetivo que analiza los riesgos que enfrenta una organización se basa en la experiencia, el juicio y la intuición.

Caballero (2013) afirma que el análisis cualitativo es un método analítico que no asigna valores numéricos a las amenazas, sino que opta por la categorización general por niveles de gravedad. La clasificación del riesgo se determina por la experiencia y el conocimiento de las personas que realiza la evaluación.

Bistarelli et al. (2006) indica que el análisis cualitativo evalúa el nivel de riesgo de un sistema utilizando una variedad de técnicas tales como sondeo, entrevista y cuestionario con el propósito de clasificar los activos y las amenazas según la gravedad del riesgo y la probabilidad de que ocurra.

Evalúa el nivel de riesgo de seguridad de un sistema de TI utilizando una variedad de técnicas de sondeo, entrevista y cuestionario con el objetivo de clasificar comparativamente los activos y amenazas según su criticidad y probabilidad percibidas, respectivamente. Por lo general, adoptan el análisis de escenarios, que requiere la construcción de diferentes escenarios de

vulnerabilidad informática, con el fin de ilustrar cuán vulnerable es una organización a los ataques asociados a tecnología de la información

Un tipo particular de instrumentos que pueden utilizarse para realizar un análisis de escenarios son los árboles de ataque. Los árboles de ataque proporcionan una manera formal y metódica de describir cómo se pueden realizar los ataques contra un sistema y mezclan técnicas cualitativas y cuantitativas.

Un escenario de ataque se puede representar en una estructura de árbol cuya raíz es el objetivo del atacante y las rutas desde los nodos hoja hasta la raíz representan las diferentes formas de lograr este objetivo. La raíz del árbol está asociada con el activo del sistema de TI a ser estudiado o con el objetivo de un respectivo ataque, Los nodos hoja representan interacciones entre el atacante y la victima para conseguir un objetivo simple que llevan al atacante a dañar (parcialmente) el activo mediante la explotación de una vulnerabilidad o avanzar en el proceso del ataque en sí mismo.

3.3.2. Tipos de Análisis Cualitativo. A continuación, se explica algunos tipos de análisis cualitativo:

*3.3.2.1. Matriz de riesgo.* Albanese (2012) señala que la matriz de riesgo es un instrumento que busca cuantificar cada uno de los riesgos con el propósito de disminuir el grado de subjetividad al momento de realizar la evaluación de los riesgos graves y menores para determinar la probabilidad de que ocurra y el impacto que genera la amenaza. De esta manera se podrá establecer una categorización para cada uno de los riesgos en los niveles bajo, moderado y alto. En este caso a cada uno se les asigna un color para poderlos reconocer con facilidad, generalmente el nivel de riesgo bajo es representado con el color (verde), el medio (amarillo) y el alto (rojo). Los niveles de gravedad pueden variar dependiendo de la forma en la cual se realice la matriz de riesgo.

*3.3.2.2. Análisis de pajarita.* El análisis de pajarita analiza el evento del riesgo luego lo proyecta en dos direcciones. A la izquierda, enumera todas las posibles causas de un evento, a la derecha enumera todas las posibles consecuencias del evento. Con este método simple se puede identificar y aplicar tratamientos a cada una de las causas y consecuencias por separado. Esto ayuda a abordar ambos lados de un riesgo al mitigar la probabilidad de que ocurra en un lado, al tiempo que limita el impacto.

*3.3.2.3. Técnica Delphi.* Regante & Torrado (2016) afirman que la técnica Delphi consiste que expertos en ciberseguridad responden a varios cuestionarios. Las respuestas se agregan y se comparten con el grupo después de cada ronda. Esta técnica se puede aplicar tanto para identificar el riesgo como posteriormente para evaluar la probabilidad y el impacto. Se pide a los expertos que opine sobre la probabilidad de que ocurra el riesgo y las consecuencias de la ocurrencia. Estas respuestas son agregadas y revisadas hasta que se logre un consenso.

*3.3.2.4. Análisis WIF.* El análisis WIF aplica un enfoque sistemático que analiza los riesgos en un entorno de taller. Los equipos investigan cómo los cambios de un plan aprobado pueden afectar el proyecto a través de una serie de consideraciones de ¿Qué pasaría sí? Esta técnica es particularmente útil para evaluar la viabilidad de los riesgos de los diferentes escenarios.

*3.3.2.5. Principio de Pareto.* Barroso (2007) señala que el principio de Pareto se conoce como regla 80/20 porque la tesis principal sostiene que el 80% de los logros obtenidos se originan en el 20% del esfuerzo. Las organizaciones utilizan el análisis de Pareto para determinar que el 20% de las causas son las que provocan el 80% de los riesgos, es decir, si soluciona el 20% que provoca el riesgo se resuelve el 80% de las amanezcas existentes por lo tanto se reduce los riesgos.

*3.3.2.6. Diagrama de causa y efecto.* Es una herramienta de análisis de proyecto que permite representar un problema y sus posibles causas de manera visual, más conocida como la

espina de pescado. El diagrama de causa y efecto es una herramienta que ayuda orientar en la toma de decisiones al abordar las razones por las cuales hay un desempeño deficiente dentro de las mismas. Para realizar este tipo de diagrama lo primero que se debe hacer es dibujar una línea horizontal que apunte hacia la derecha y se procede a escribir el problema dentro de un rectángulo, triangulo o circulo que ubique en la punta de la flecha, luego se identifica las principales causas que generan la problemática. Se recomienda que una vez se haya realizado el diagrama se revise de nuevo, para identificar si faltan causas por agregar o bien si es necesario descarta ciertas causales, se selecciona las más relevantes para determinar el grado de incidencia. Este diagrama es muy utilizado por las empresas porque le permite conocer las problemáticas y las amenazas para después plantear soluciones.

*3.3.2.7. Árbol de eventos.* Hernández, Díaz & Fernández (2006) mencionan que el árbol de eventos (Grafos de ataque) es una ilustración grafica en la que se registran una secuencia de eventos en la que se realiza una evaluación de la probabilidad de las fallas o cualquier tipo de evento que puedan causar daños a los activos de la organización. Para realizar el árbol de eventos es necesario identificar las causas que originaron la amenaza seleccionando cada respuesta como positiva o negativa.

*3.3.2.8. Análisis de fallo y efectos.* Herráez & Acuña (2009) lo definen como un procedimiento que analiza las causas y los efectos que podrían provocar las fallas en un determinado producto o servicio busca identificar todas las causas para luego realizar acciones de prevención. Este análisis está conformado por tres etapas: la ocurrencia, la gravedad y la detección. En la ocurrencia se examina la probabilidad de que un fallo ocurra, en la etapa de gravedad se mide los efectos del fallo y en la detección busca evitar los riesgos o amenazas mediante medidas

de ciberseguridad. Al ser un análisis de método cualitativo, hace que el procedimiento sea determinado bajo la consideración del personal de la empresa.

*3.3.2.9. Análisis de escenarios.* El análisis de escenarios tiene como finalidad analizar dos puntos de vista el atacante y el defensor para determinar cómo procede cada una de las partes. A continuación, se menciona dos tipos de metodologías que permite identificar cada uno de los escenarios mediante árboles de ataque y árboles de defensa:

*3.3.2.9.1. Metodología de árbol de ataque.* Según Bistarelli et al. (2006) la metodología de árbol de ataque tiene por objeto conocer las vulnerabilidades del sistema de la víctima, para luego identificar las principales rutas de acceso que puede utilizar los ciberdelincuentes para poder ingresar a la información confidencial o afectar los activos de la organización. Los árboles de ataque es una herramienta que le permite esquematizar a las empresas una representación visual a escala de un posible escenario de ataque. Permite incluir dentro del análisis variables de comportamiento de la víctima y del atacante.

Los árboles de ataque determinan cómo un atacante realiza ataques contra un sistema. Un escenario de ataque se puede representar en una estructura de árbol cuya raíz es el objetivo del atacante y las rutas son los nodos de las hojas hasta la raíz representan las diferentes formas de lograr el objetivo (escenarios). La raíz del árbol está asociada con el activo de la organización objeto del ataque. Los nodos de la hoja representan los sub objetivos que llevan al atacante causar daño al activo mediante la explotación de una vulnerabilidad. Los nodos que no son hojas incluida la raíz del árbol representan una estrategia de ataque, bien sea un nodo OR (alternativas) o un nodo AND (describen procesos).

*3.3.2.9.2. Metodología de árbol de defensa.* Bistarelli et al (2006) definen la metodología de árbol de defensa como una técnica que consiste en crear una gran cantidad de contramedidas

en las hojas del árbol, creando mecanismos de protección que mitiguen los posibles ataques. Así como también afirma que a través de la metodología de los árboles de defensa se puede determinar si una protección en ciberseguridad vale la pena ser financiada o no e incluso evalúa la efectividad de las medidas de protección, el monto de pérdidas o ganancias que podría generar las contramedidas a utilizar.

3.3.3. Proceso del Análisis Cualitativo. Según Gregg (2007) para hacer un análisis cuantitativo, tradicionalmente, se debe seguir los siguientes pasos:

*3.3.3.1. Paso 1: Identificar los riesgos.* Paz & Rozenboim (2014) señalan que el primer paso en el análisis cualitativo es identificar los riesgos, como primera medida se debe hacer un inventario de cada uno de los activos de la organización para esta manera conocer los principales puntos débiles o vulnerabilidades o fallas técnicas que hacen a los sistemas o la infraestructura critica más propensa a los ataques cibernéticos. Ya teniendo esta información se procede clasificar los riesgos por niveles como muy alto, alto, bajo y muy bajo. Los riesgos pueden ser muy amplios por lo tanto es fundamental delimitar los riesgos que tienen más probabilidad de ocurrir. Para desarrollar este paso se puede utilizar las siguientes herramientas:

- Mapas mentales.
- Cuestionarios.
- Entrevistas.
- Revisión de documentación.
- Análisis de lista de verificación.
- Análisis FODA.

*3.3.3.2. Paso 2: Estimar la probabilidad.* Gregg (2007) dice que el segundo paso es estimar la probabilidad. Para esta parte del análisis, solo se tiene en cuenta la probabilidad de que se

materialice el riesgo, no la naturaleza o el alcance de los daños que podría causar. Para estimar la probabilidad se debe realizar los siguientes ejercicios:

- Hacer una escala de cuatro puntos que especifique muy improbable a muy probable para poder medir la probabilidad.
- Asignar valores, escalas o porcentajes a la probabilidad para determinar la gravedad o complejidad del riesgo. Por ejemplo, puede asignar una puntuación del 20% a muy improbable, 40% a improbable, 60% a probable y 80% a muy probable.

Teniendo en cuenta que la probabilidad de un ataque depende de la facilidad del ataque y de la motivación del atacante una manera más precisa es utilizar los modelos matemáticos derivados del uso de los ÁRBOLES DE ATAQUE.

*3.3.3.3. Paso 3: Estimar el impacto.* El siguiente paso es estimar el impacto que provoca cada uno de los riesgos que se haya identificado. En este paso, ignora la probabilidad y trata cada variable como una certeza. Para estimar el impacto se realiza lo siguiente:

- Determinar ¿Cuál es el peor daño posible que el riesgo podría causar a los activos de la organización?
- Estimar las pérdidas económicas, directas e indirectas, que provoca cada uno de los riesgos.
- Se debe tener en cuenta toda la información analizada para que las estimaciones sean lo más preciso posible.
- Una vez se identifique la amenaza se asigna una puntuación de gravedad que puede ser una escala numérica simple como 1 para impacto muy bajo, 2 para bajo, 3 para alto y 4 *para muy alto.*

*3.3.3.4. Paso 4: Crear una matriz de riesgos.* Albanese (2012) afirma que después de haber identificado los riesgos, estimar la probabilidad y el impacto todo este análisis se reúne en una

matriz de riesgo. Por lo tanto, se tiene que multiplicar las clasificaciones de probabilidad e impacto en cada fila y columna para obtener el puntaje de exposición del riesgo para cada celda de la matriz. El puntaje de exposición resume el nivel de amenaza que representan los riesgos en cada celda.

Gregg (2007) señala que para crear una matriz de riesgos se debe hacer los siguientes pasos:

*3.3.3.4.1. Configuración del grafico de la matriz de riesgo. Se debe configurar el gráfico de la matriz de riesgo para que se adapte a las necesidades de la organización. No importa qué el eje se convierta en la fila horizontal o vertical en el gráfico, o si la escala se ejecuta en orden ascendente o descendente. Una vez se haya creado la matriz, puede trazar todos los riesgos de acuerdo con las clasificaciones de probabilidad e impacto que se asignó en el análisis (Ver figura 15).*

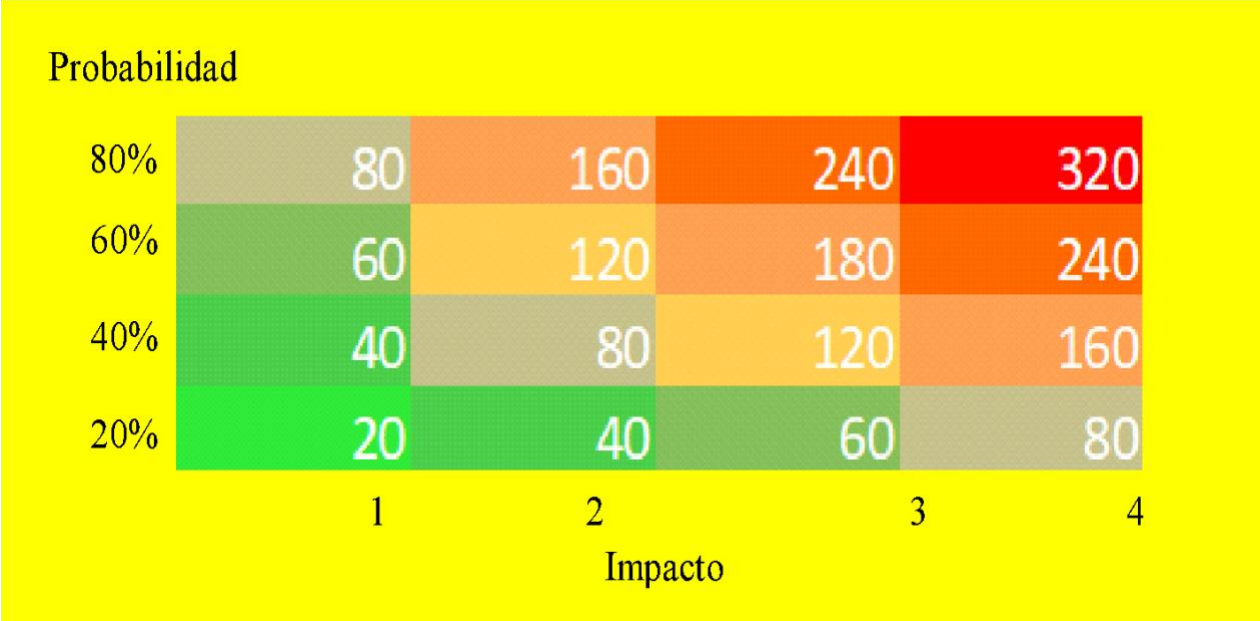



*Figura 15 Ejemplo de matriz de riesgo. Fuente: Imagen tomada de Albanese, D. (2012).*

Cada celda de una matriz de riesgo contiene una puntuación de exposición igual a la probabilidad por el impacto.

*3.3.3.4.2. Establezca niveles de exposición del riesgo.* Gregg (2007) manifiesta que cuando se realice la matriz de riesgos se debe dividir los riesgos en categorías según la gravedad o la complejidad de los mimos. Se clasifica por los siguientes niveles:

- Si el nivel del riesgo es muy alto se tendrá que contratar especialistas en ciberseguridad.
- Si el nivel de riesgo es alto se debe implementar medidas ciberseguridad para proteger los sistemas o infraestructura critica de la organización.
- Si el nivel de riesgo es bajo se realiza un monitoreo con el fin de mejorar los criterios de seguridad que tenga la empresa.
- Si el nivel de riesgo es muy bajo la organización puede seguir con los mecanismos de seguridad ya existente sin ningún inconveniente.

*3.3.3.4.3. Establecer color de exposición del riesgo.* Se debe usar colores para representar la gravedad del riesgo. El rojo se puede aplicar a los riesgos de nivel muy alto es decir que requieren una acción mayor de mitigación, el naranja a los riesgos de nivel alto que requieren de un análisis más detallado, el amarillo a los riesgos de nivel bajo y el verde a los riesgos de nivel muy bajo que son amenazas aceptables (Albanese, 2012).

*3.3.3.4.4. Tratamiento de riesgos.* Gregg (2007) establece que una vez se realice la matriz de riesgo la organización puede tratar el riesgo de la siguiente manera:

- Acepta. Si un riesgo tiene un impacto bajo y una probabilidad baja o el costo de prevenirlo no es tan alto, es rentable aceptarlo.
- Mitiga. Algunos riesgos tienen una alta probabilidad de que suceda lo que significa que no se puede evitar, por lo tanto, para reducir el impacto se mitiga el riesgo.

- Explota. Se pueden aprovechar algunos riesgos en beneficio de la organización. Tener la capacidad de identificar riesgos explotables puede ser extremadamente ventajoso y destaca la importancia de buscar expertos con experiencia que puedan detectar estas oportunidades.
- Transfiere. Los riesgos de impacto financiero son un ejemplo de riesgos que pueden transferirse a un tercero como se constituye un seguro este asume las pérdidas que llegará ocurrir. Asimismo, es posible transferir el riesgo a través de un contrato a un proveedor o contratista.
- Evita. Si no puede mitigar o transferir y el riesgo es demasiado alto para aceptarlo, el único recurso es tratar evitarlo mediante medidas de ciber-inteligencia, anticipándose al ataque, detectando la amenaza desde etapas tempranas de la cadena del "ciber kill chain".

*3.3.3.5. Paso 5: Desarrollar un plan de respuesta al riesgo.* Según Gregg (2007) una vez se conozca los resultados de la matriz de riesgo se procede hacer un plan de respuesta al riesgo para que la organización pueda defenderse ante las amenazas cibernéticas y debe preparar al personal sobre políticas de seguridad para reducir la probabilidad de los ciberataques.

### 3.4. Importancia del Análisis Cuantitativo y Cualitativo para las Organizaciones

Ochoa (2019) afirma que el análisis cuantitativo y cualitativo son procesos que ayuda a la organización identificar, evaluar y controlar las amenazas. Además, optimiza las ganancias y mitiga el daño que puede causar los ataques cibernéticos y permite a las empresas prepararse para lo inesperado minimizando los riesgos y los costos antes de que sucedan. Estas metodologías son importantes porque les otorga herramientas a las empresas para tratar adecuadamente los riesgos. Según Holtsnider & Jaffe (2012) por medio del análisis cuantitativo y cualitativo la organización:

3.4.1. Previene los Riesgos Cibernéticos. A través del análisis cuantitativo y cualitativo la organización identifica riesgos cibernéticos, evalúa la probabilidad en caso que ocurra, determina la perdida que provoca el ciberataque y calcula los costos de prevención del riesgo. Con base a esta evaluación la empresa procede implementar medidas de ciberseguridad acorde con la capacidad económica de la empresa.

3.4.2. Reduce Costos. Cuando la organización realiza el análisis cuantitativo y cualitativo se reduce costos pues gracias a esta evaluación se puede hacer pronósticos acerca de la probabilidad del ataque y la perdida que causa la amenaza cibernética e incluso se puede conocer cuánto vale una medida de protección. Con base a esta información las empresas realizan medidas de ciberseguridad más efectivas que están basadas en un análisis que identifica el riesgo antes que ocurra el ataque cibernético.

3.4.3. Mejora la Reputación de la Organización. Demostrar a los clientes que se toma en serio la seguridad cibernética le da a la organización una ventaja competitiva. Las organizaciones que priorizan los datos de los clientes ganan confianza y obtienen como resultando lealtad por parte de los clientes y tiene un mayor éxito comercial.

Al no poder evaluar de manera efectiva las consecuencias de las decisiones de inversión en seguridad de la información, los gerentes solo pueden especular sobre su costo-beneficio. Desgraciadamente, dicha inversión se podrá valorar cuando se materialice ataque. Algunos gerentes lo toman como un seguro. El modelo de evaluación de la relación costo/beneficio de los diferentes puntos de control (Contramedidas), debe ser capaz de captar las complejidades de la decisión de seguridad, ya que involucra variables probabilísticas que miden el comportamiento de un atacante y la explotación de vulnerabilidades del sistema de defensa. Contar con una metodología que permita describir la forma como podría llevarse a cabo un ataque, al tiempo que

permite una exploración sistemática del riesgo mitigado de las diferentes opciones de contramedidas de ciber-seguridad, usando Árboles de Ataque, serviría como herramienta de ayuda a los gerentes de seguridad para soportar sus decisiones de priorización de inversión, más allá de la subjetividad de la experiencia o la asesoría de los vendedores de equipos de ciberseguridad.

Los árboles de ataque es una herramienta para analizar situaciones complejas, son mucho más que una descripción de un ataque (Árbol de Grafos) ya que introducen dentro del análisis variables asociadas al atacante. Es importante entender que para que se produzca un ataque se debe cumplir las siguientes tres condiciones:

- Exista una vulnerabilidad
- Que haya un atacante motivado.
- Que el atacante tenga los recursos (técnicos, económicos) para aprovechar las vulnerabilidades y realizar el ataque.

La primera condición está bajo control de los responsables de ciberseguridad de una organización, las otras dos dependen del atacante.

La seguridad digital se está convirtiendo cada vez más en un tema importante dentro de la agenda de los líderes de las organizaciones. Los ciberataques realizados en una organización influyen en su rendimiento y economía. Los aspectos económicos incluyen márgenes de ganancia, capitalización de mercado e imagen de marca de la organización ( Mukhopadhyay et al, 2013). Los humanos siguen siendo el eslabón más frágil de la ciberseguridad. También deben tenerse en cuenta las capacidades de las personas. Los ciberataques típicos incluyen los siguientes (Roumani et al, 2015):

- Denegación de servicios;

- Ramsomware
- Virus, gusanos informáticos y caballos de Troya;
- Ataques basados en web;
- Etc.

La seguridad de la información tiene un ciclo de vida que describe un ciberataque. Un ataque de un adversario suele estar dirigido al sistema de información de la organización. Una brecha ocurre cuando el ataque penetra y compromete el sistema de información. La recuperación ocurre cuando la pérdida es limitada y la organización puede volver a la primera etapa de defensa contra ataques. Las organizaciones recurren al uso de dispositivos tecnológicos en múltiples niveles de seguridad para reducir la frecuencia y gravedad de una brecha de seguridad (Mukhopadhyay et al, 2013, Behara et al. 2007)

Ciber-Seguridad consiste en el desarrollo de un ecosistema de protección para reducir los riesgos de las amenazas que existen en el ciberespacio. Esto involucra la revisión dentro de la organización de los procesos, personas y tecnologías. incluye perspectivas de seguridad preventiva, de detección y correctiva. La defensa eficaz depende de la selección de estrategias adecuadas de gestión de la seguridad entre las diferentes opciones disponibles, cada una con diferentes costos y beneficios potenciales. Es necesario contar con una metodología que permita a los gerentes tomar decisiones con base un análisis económico de las diferentes contramedidas.

### 3.4.5 Metodología para evaluación ROSI usando Árboles de ataque.

El riesgo cibernético incluye la posibilidad de que una amenaza cause la interrupción de las operaciones, así como una pérdida monetaria. Afecta los resultados de una organización con pérdida de costo de oportunidad debido a un impacto adverso en el valor de la marca y la capitalización de mercado (Mukhopadhyay et al, 2013). Las organizaciones deben decidir cuántos

recursos deben invertir en ciberseguridad para minimizar las pérdidas debidas a los ciberataques (Roumani et al, 2015). La cantidad invertida en ciberseguridad es una decisión estratégica. Esta decisión debe basarse en un análisis de costo-beneficio para garantizar que los riesgos se aborden de manera adecuada (Mukhopadhyay et al, 2013). La posibilidad de un riesgo se materialice tienen un impacto directo en una organización en términos de pérdidas en los resultados, valor de marca y capitalización de mercado.

A la gerencia ejecutiva realmente no le importa que el sistema de detección de intrusiones (IDS) o el firewall protejan los servidores de la organización. En cambio, están más preocupados por conocer el impacto de tales medidas de seguridad en los resultados financieros finales. Es importante tener en cuenta que las inversiones en seguridad no se pueden traducir directamente en beneficios monetarios, pero pueden evitar pérdidas comerciales considerablemente. Por lo tanto, para describir la importancia de la inversión en seguridad, es esencial demostrar el impacto de la falta de mecanismo de seguridad sobre la productividad, o sobre la imagen de marca, o sobre las ventas, etc. Es decir, es importante identificar las variables económicas que se verían afectadas en caso de que se materialice un ataque. Por ejemplo, para el caso de un ataque de Denegación de servicios a una universidad, la percepción de dolor de estar fuera de servicio, es diferente que, para una tienda virtual, en el día sin IVA. Ver figura 13. Es importante que los gerentes de seguridad expliquen la gravedad de la brecha de seguridad con respecto a una pérdida potencial para la organización. ROSI (Retorno de la inversión en Seguridad) es un enfoque eficaz para justificar tales inversiones, ya que ayuda a priorizar cual es la solución rentable, cual es la cantidad correcta de dinero para invertir en seguridad. Impacto de la inversión en seguridad en las palancas de valor de una organización.

Según YAQOOB (2019) Existen numerosas metodologías de ROSI para ayudar a los tomadores de decisiones, pero plantean grandes desafíos en el dominio de la seguridad cibernética. Estos marcos carecen de algunos insumos importantes que se requieren especialmente para la inversión en seguridad cibernética. Una de las limitaciones es que estos marcos no calculan matemáticamente la probabilidad de una amenaza particular, sino que la probabilidad de que ocurra un ataque suele estar determinada por las experiencias y la exposición de los empleados. Por lo tanto, la aproximación confiable del riesgo utilizando Árboles de ataque es un desafío, ya que las organizaciones generalmente terminan obteniendo resultados diferentes incluso en las mismas condiciones descritas en un árbol de ataque, ya que la tolerancia al riesgo de cada organización es diferente. La curva de percepción de dolor cambia entre víctima y víctima. .

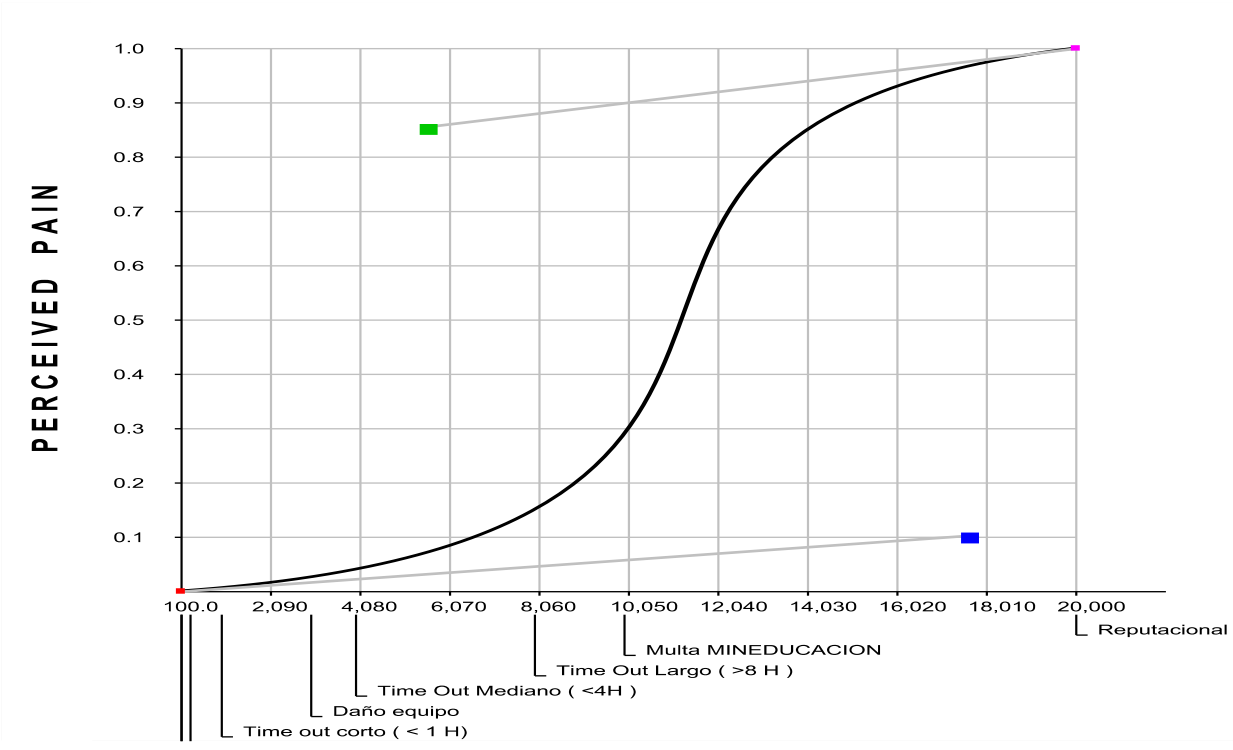



*Figura 16 Normalización de la percepción de Dolor para una universidad frente a un ataque DoDS. Elaboración propia. . SecurITree V 5.2*

La Figura 16. nos indica que esta víctima, su percepción de dolor se incrementa después de una falla fuera de servicio superior a 10 horas. Lo cual puede diferir de otra víctima donde su dolor se incrementa exponencialmente después de estar 2 horas fuera de servicio. Esta forma como cada uno percibe el dolor, determina su comportamiento frente a una amenaza y define su perfil de riesgo.

Este trabajo de grado propone un marco para calcular ROSI de las contramedidas implementadas en ciberseguridad, superando las lagunas en la literatura existente. Nuestra metodología propuesta calcula el impacto de un ataque en todo el negocio considerando su efecto sobre todos los activos críticos e incluye una normalización de la curva de dolor entre 0 y 1 (Ver Figura 16 donde tratamos de reflejar diferentes impactos dependiendo del ataque recibido). Para determinar la probabilidad de un ciberataque, hemos utilizado ARBOL DE ATAQUES, ya que aproximaciones matemáticas más precisas como el teorema Bayes exige disponibilidad de información que para muchas compañías y entidades son de difícil acceso y complejas de entender. La metodología de los Árboles de ataque está bien establecida y probada en el proceso de análisis de Riesgos desde hace más de 20 años. Su inclusión en la estimación del Riesgo mitigado, debido a la introducción de una contramedida, será muy útil y productiva si se aplica correctamente

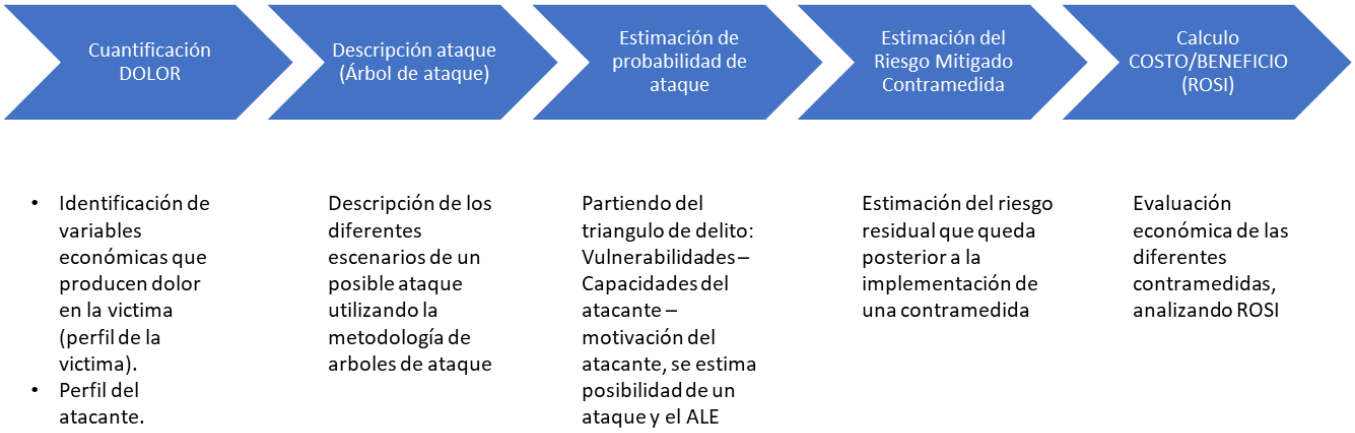



*Figura 17. Metodología del autor propuesta de evaluación económica de inversiones en ciberseguridad. Elaboración propia.*

Para justificar sistemáticamente las inversiones en seguridad, en esta sección se ha propuesto un marco ROSI basado en Árboles de ataque. El modelo propuesto consta de cinco fases importantes, como se ilustra en la Fig. 17. La primera fase trata sobre la valoración de impacto, identificando las variables que más le causan dolor a la víctima en caso de que un ataque se llegara a presentar. Ayuda a identificar que tanto dolor está dispuesto a soportar una víctima desde el punto de vista del directivo (tomador de la decisión). También en esta fase se construye el perfil del atacante (habilidades técnicas y recursos disponibles para realizar el ataque). El segundo paso consiste en una descripción de todos los escenarios de un posible ataque, desde la perspectiva del atacante, utilizando la metodología de los Árboles de ataque. La tercera fase está relacionada con el cálculo de la posibilidad de que un ataque suceda teniendo en cuenta de que existe una vulnerabilidad, que existe un atacante dispuesto aprovechar dicha vulnerabilidad con recursos económicos y técnicos para llevarla a cabo y lo más importante esta suficiente motivado, por el beneficio que dicho ataque conlleva. Esta fase también determinará la pérdida anual de una

organización en caso de que se explote la vulnerabilidad y se materialice el ataque (ALE). La cuarta fase trata sobre el cálculo del Riesgo residual, que permanece después de la inclusión de posibles contramedidas que puedan mitigar la materialización de la amenaza. Ayuda a analizar la eficacia de estas contramedidas desde la perspectiva del Riesgo mitigado. La siguiente fase tiene que ver con el cálculo de ROSI. Para ello, se realiza un análisis de costo-beneficio, teniendo en cuenta la perdida que cubre

### 3.5. Estimación del riesgo utilizando Árboles de ataques.

Según Terry (2021), los ataques se pueden modelar usando una estructura de árbol de decisión gráfica y matemática llamada árbol de ataque. Hay razones para creer que los árboles de ataque se originaron en la comunidad de inteligencia. Se cree que al menos una agencia de inteligencia utilizó técnicas de modelación de ataques basadas en árboles a fines de la década de 1980.

Prerrequisitos para un ataque

Deben estar presentes tres condiciones para que un atacante (también conocido como agente de amenaza) realice un ataque contra el sistema de un defensor.

El defensor debe tener vulnerabilidades o debilidades en su sistema.

El agente de amenaza debe tener suficientes recursos disponibles para explotar las vulnerabilidades del defensor. Esto se conoce como capacidad.

El agente de amenaza debe creer que se beneficiarán al realizar el ataque. La expectativa de beneficio impulsa la motivación.

La condición 1 depende completamente del defensor.

La condición 2 depende tanto del defensor como del agente de amenaza para cumplirse.

El defensor tiene cierta influencia sobre qué vulnerabilidades existen y qué nivel de recursos se necesitarán para explotarlas. Diferentes agentes de amenaza tienen diferentes capacidades.

La condición 3 involucra principalmente al atacante. Representa la motivación para llevar a cabo el ataque. El defensor puede tener un papel si sus acciones provocan que un agente de amenaza realice un ataque.

El agente de amenaza y el defensor interactúan para determinar conjuntamente si ocurre un ataque. El análisis de ataque adecuado requiere que examinemos las tres condiciones para predecir el comportamiento de los adversarios y la probabilidad de que ocurra un ataque.

Comprender estos factores también proporciona información sobre formas efectivas de prevenir ataques.

Los árboles de ataque se construyen desde el punto de vista del adversario. Crear buenos árboles de ataque requiere que pensemos como un atacante. No nos centramos en cómo defender un sistema cuando creamos inicialmente el modelo. En cambio, pensamos en lo que un atacante quiere lograr y las formas de lograrlo. Más tarde, usamos la comprensión que hemos adquirido de las vulnerabilidades del sistema para mejorar sus defensas.

Como la mayoría de los modelos de árboles matemáticos, los árboles de ataque están representados por un diagrama con un solo nodo raíz en la parte superior. La raíz se ramifica hacia abajo, expandiéndose a través de horquillas y más ramas. Esto es similar a los árboles de decisión utilizados para ayudar con las decisiones comerciales o los árboles de fallas utilizados para comprender la fiabilidad de las máquinas y los procesos similares a las máquinas.

En un modelo de vulnerabilidad de árbol de ataque, el nodo superior (raíz) representa un objetivo que sería beneficioso para uno o más agentes de amenaza. Desafortunadamente, el logro del objetivo raíz generalmente trae consecuencias negativas para el defensor. Si el objetivo se elige cuidadosamente, generalmente es posible analizar un sistema completamente con un solo árbol de ataque. En algunas situaciones, un adversario en particular puede tener varios objetivos diferentes, o diferentes adversarios pueden tener sus propios objetivos únicos.

En ocasiones, estas situaciones requieren múltiples árboles de ataque para llevar a cabo un análisis completo.

Por sí mismo, el objetivo raíz es tan elevado o tan amplio que da poca comprensión de cómo se puede lograr. Es útil dividir el objetivo raíz de alto nivel en pasos más pequeños y manejables. Esto permite formular una serie de estrategias diferentes que podrían alcanzar el objetivo general. Estas estrategias pueden expresarse como una serie de objetivos intermedios que individualmente, o en combinación, logran el objetivo raíz. Este proceso de descomposición continúa, rompiendo los objetivos intermedios en actividades cada vez más finas. Esto se representa convenientemente usando un formato gráfico (ver Figura 18).

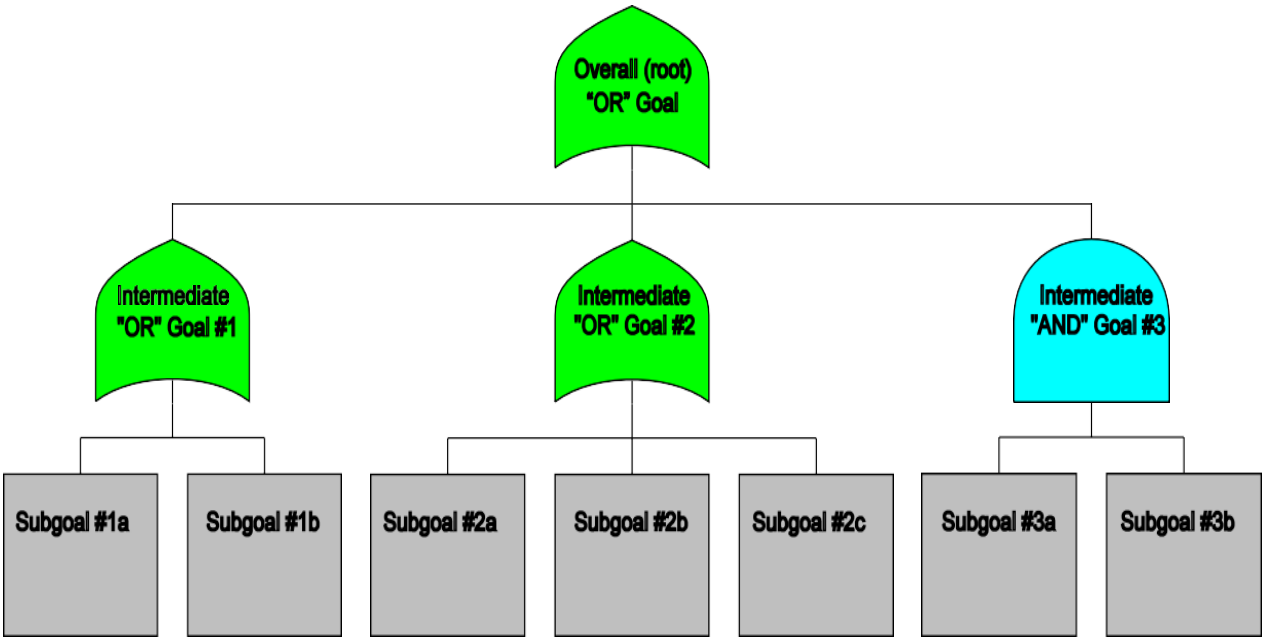



*Figura 18 Descripción de los componentes de un ARBOL DE ATAQUES. Terry (2021)*

El símbolo superior del árbol representa el objetivo general del adversario. Se conoce como la raíz del árbol. La raíz en este ejemplo particular se representa con un símbolo verde con la parte superior puntiaguda. El diagrama muestra cómo los objetivos de alto nivel se descomponen en submetas cada vez más precisas a medida que descendemos a través del árbol.

El símbolo “OR” (cuya forma debería ser familiar para los lectores familiarizados con el álgebra Booleana) indica que el objetivo general "OR" raíz se puede lograr al alcanzar el objetivo intermedio #1 “OR” Intermedio #2 “OR” Intermedio #3. Los hijos de los nodos “OR” representan las formas alternativas en que se puede alcanzar el objetivo secundario “OR”.

En este ejemplo, los nodos OR en la figura se dividen aún más en formas rectangulares, llamadas nodos hoja. Por ejemplo, el objetivo intermedio "OR" # 1 se puede lograr al alcanzar el objetivo secundario # 1a (Subgoal #1a) OR el objetivo secundario # 1b (Subgoal #1b). Los nodos

hoja representan actividades atómicas que no requieren más divisiones para ser entendidas. Representan actividades que podría realizar un atacante.

El Objetivo Intermedio #3 está representado por un símbolo “AND” y cian. Esto indica que el Objetivo Secundario #3a Y (AND) el Objetivo Secundario #3b deben completarse para alcanzar el Objetivo Intermedio #3. Los hijos de los nodos "AND" representan una serie de pasos en un proceso o procedimiento que debe realizarse para alcanzar o satisfacer el nodo "AND".

Estrictamente hablando, el orden de los hijos de AND no tiene importancia. Sin embargo, una convención útil es que, si el orden es importante para el logro del nodo AND, los hijos se organizan en orden gradual de izquierda a derecha. (Terry, 2021)

Un ejemplo aclarará esto.

Supongamos un ataque de denegación de servicios. El objetivo del ataque es causar una indisponibilidad en un servicio que ofrezca una plataforma informática por un periodo de tiempo. Ese será el nodo Raíz. Después de consultar con expertos podemos ver (Figura 4) que hay tres alternativas posibles para lograr el objetivo:

Ataque a los servidores

Ataque al sistema de comunicaciones

Ataque al nivel de la aplicación.

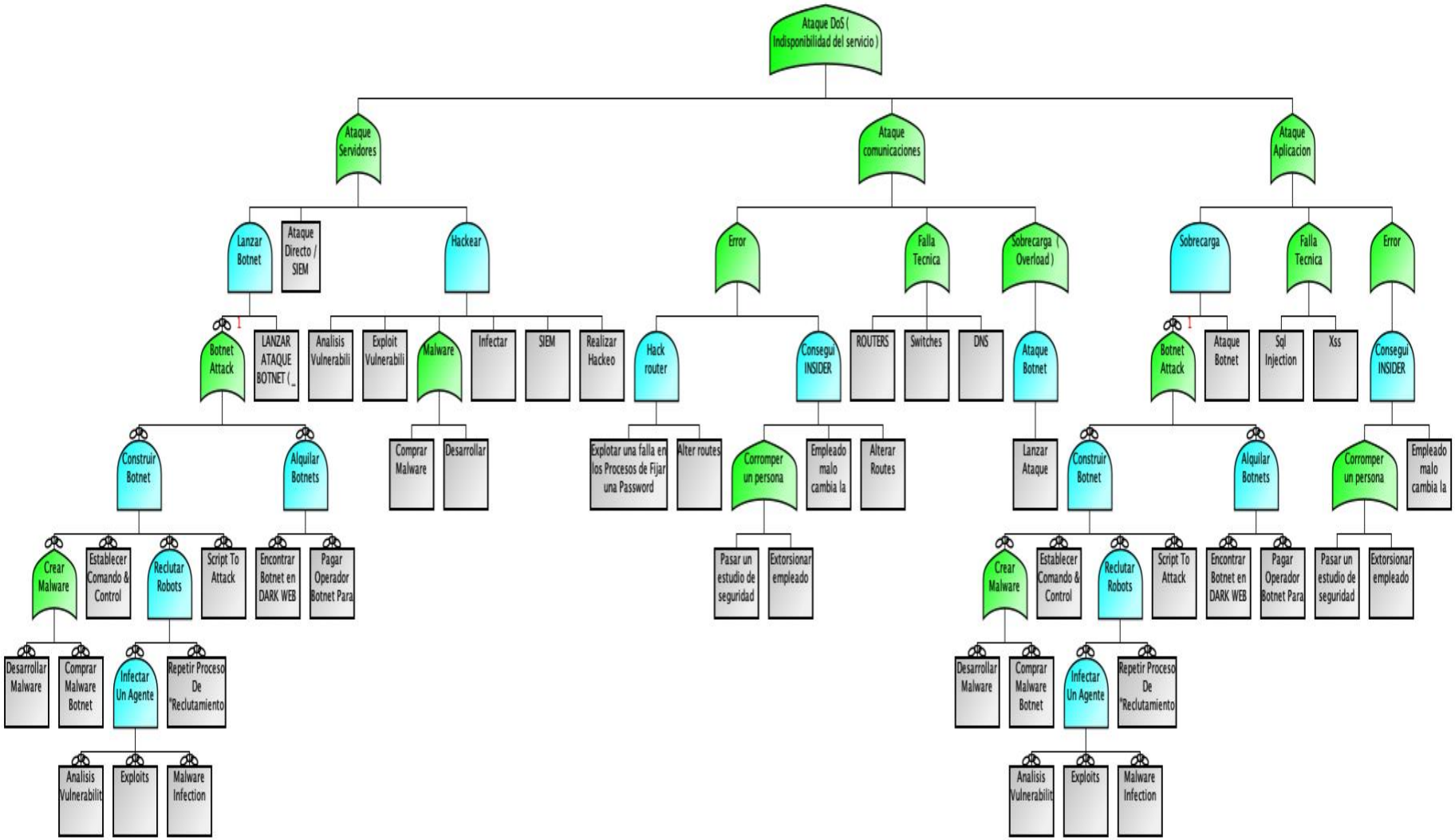

Ataque DoS ( Indisponibilidad del servicio )
Ataque Servidores
Ataque comunicaciones
Ataque Aplicacion
Lanzar Botnet
Ataque Directo / SIEM
Hackear
Error
Falla Tecnica
Sobrecarga ( Overload )
Sobrecarga
Falla Tecnica
Error
Botnet Attack
LANZAR ATAQUE BOTNET ( _
Analisis Vulnerabili
Exploit Vulnerabili
Malware
Infectar
SIEM
Realizar Hackeo
Hack router
Consegui INSIDER
ROUTERS
Switches
DNS
Ataque Botnet
Botnet Attack
Ataque Botnet
Sql Injection
Xss
Consegui INSIDER
Construir Botnet
Alquilar Botnets
Comprar Malware
Desarrollar
Explotar una falla en los Procesos de Fijar una Password
Alter routes
Corromper un persona
Empleado malo cambia la
Alterar Routes
Lanzar Ataque
Construir Botnet
Alquilar Botnets
Corromper un persona
Empleado malo cambia la
Crear Malware
Establecer Comando & Control
Reclutar Robots
Script To Attack
Encontrar Botnet en DARK WEB
Pagar Operador Botnet Para
Pasar un estudio de seguridad
Extorsionar empleado
Crear Malware
Establecer Comando & Control
Reclutar Robots
Script To Attack
Encontrar Botnet en DARK WEB
Pagar Operador Botnet Para
Pasar un estudio de seguridad
Extorsionar empleado
Desarrollar Malware
Comprar Malware Botnet
Infectar Un Agente
Repetir Proceso De "Reclutamiento
Desarrollar Malware
Comprar Malware Botnet
Infectar Un Agente
Repetir Proceso De "Reclutamiento
Analisis Vulnerabilit
Exploits
Malware Infection
Analisis Vulnerabilit
Exploits
Malware Infection

*Figura 19 ARBOL DE UN ATAQUE DDOS. Elaboración propia usando la herramienta SecurITree @amenaza*

Cada alternativa se convierte en un escenario en u escenario independientemente probable. Vamos desglosar la alternativa del ataque a servidores.

Como se puede ver la Figura 19, el ataque a los servidores se puede dar por básicamente tres alternativas:

- Botnet
- Hackear
- Ataque directo desde un insider.

Para ejecutar un ataque mediante BOTNET, este se puede hacer bien sea construyendo un BOTNET o Comprando un BOTNET.

Poco a poco vas construyendo la descripción de cómo se pude producir el ataque, cada alternativa se convierte en un escenario posible de para efectuar el ataque. Esta es la primera fase de la metodología de Árbol de ataques y al defensor le ayuda a entender cómo podría producirse un ataque. En esta fase del proceso no hemos podido responder cual es la probabilidad de que un ataque se produzca. Ahora debemos incluir dentro del análisis del riesgo de un ataque, variables de comportamiento del atacante. Las variables de comportamiento son una extensión de los grafos de ataque, qué pretender describir las capacidades del atacante (recursos económicos y técnicos) y la motivación del atacante; De esa forma podemos complementar nuestro análisis para tratar de calcular cual es la probabilidad de que un ataque se produzca.

Según Terry (2021) la propensión es una medida de probabilidad de un ataque dado que, existe una vulnerabilidad, es decir, existe una oportunidad para que un agente hostil realice un

ataque y logre a través de los escenarios descritos en el árbol de ataques, llegar al nodo raíz. La métrica se basa es la combinación de dos variables: Facilidad del ataque y los beneficios que obtenga.

Probabilidad de un ataque = facilidad del ataque x beneficio del atacante.

El riesgo hostil se acepta generalmente como la combinación de dos factores:

$$Riesgo\ de\ ataque\ \equiv probabilidad\ de\ ataque\ x\ Impacto\ a\ la\ victima$$

Para comprender completamente el riesgo, nuestro modelo debe incluir el impacto que cada escenario de ataque tendrá en el defensor. Esto se puede lograr mediante una simple extensión hecha al modelo de árbol de ataque que adiciona en cada interacción entre el atacante y la victima cual podría ser el impacto para la victima de dicha interacción.

El impacto puede ocurrir en cualquier nivel del árbol. Aunque algunos impactos a las víctimas pueden ocurrir potencialmente cuando un atacante desarrolla un "exploit" (en un nodo de hoja), los impactos generalmente se hacen más grandes a niveles más altos en el árbol. Por ejemplo, las empresas a menudo no se ven afectadas por el daño menor a los sistemas informáticos que es el resultado inmediato de las actividades de un pirata informático. Sin embargo, pueden experimentar pérdidas graves o catastróficas debido a las consecuencias indirectas a medida que los sistemas comerciales no estén disponibles o se divulgue información. Para calcular el riesgo, primero analizaremos como como se calcula la probabilidad de un ataque y después calcularemos el impacto, usando Árboles de ataque.

### 3.5.1. Cálculo de la probabilidad

Según Terry (2021), para calcular la probabilidad de ocurrencia de un ataque debemos calcular la propensión de ataque de cada escenario. La posibilidad de un ataque depende del grado de facilidad que dicho ataque implica y de los beneficios que obtenga el atacante en cada escenario. Todos los días, las personas (buenas y malas) se enfrentan a elecciones y consecuencias. Es nuestra hipótesis que las personas generalmente seleccionan una actividad sobre otra porque creen que tiene una relación costo-beneficio superior a las alternativas de la competencia. Sin embargo, no es suficiente analizar los costos brutos asociados con sus elecciones. Nuestros modelos deben reflejar el hecho de que diferentes personas (ya sean atacantes o defensores) perciben valores diferentes para la misma cantidad de la misma mercancía. Es decir, la probabilidad de un ataque depende del comportamiento del atacante, depende de que tan fácil se puede realizar un ataque y de cuál será el beneficio que reciba de dicho ataque. Según el perfil del atacante, este podría decidir realizar o no un ataque, ya que, por ejemplo, para un hacker amateur realizar un ataque de denegación de servicios poder ser más difícil que para un Hacker profesional.

#### 3.5.1.1. Facilidad de ataque

Cada ataque requiere que el adversario gaste una variedad de recursos. El analista elige tipos específicos de recursos para incluir en el modelo de árbol de ataque en función del grado en que influyen en la capacidad del adversario de completar los diversos escenarios de ataque. Estos recursos pueden incluir dinero, materias primas, talento, tiempo y una buena disposición para ser notado.

Aunque todos puedan verse obligados a gastar la misma cantidad de recursos para realizar un ataque específico, eso no significa que estén igualmente dispuestos o sean capaces de hacerlo. La disponibilidad de recursos varía. Por ejemplo, un pirata informático juvenil relativamente pobre podría considerar que $1000 son de un valor considerable y estar muy poco dispuestos a

desprenderse de él sin un beneficio sustancial. Por otro lado, un ejecutivo ocupado en una gran empresa podría considerar $1000 como cambio de bolsillo. Sin embargo, el trabajador de cuello blanco con poco tiempo estaría mucho menos dispuesto a desprenderse de 25 horas de su precioso tiempo que el adolescente aburrido que está feliz de pasar las primeras horas tratando de descifrar un sistema informático.

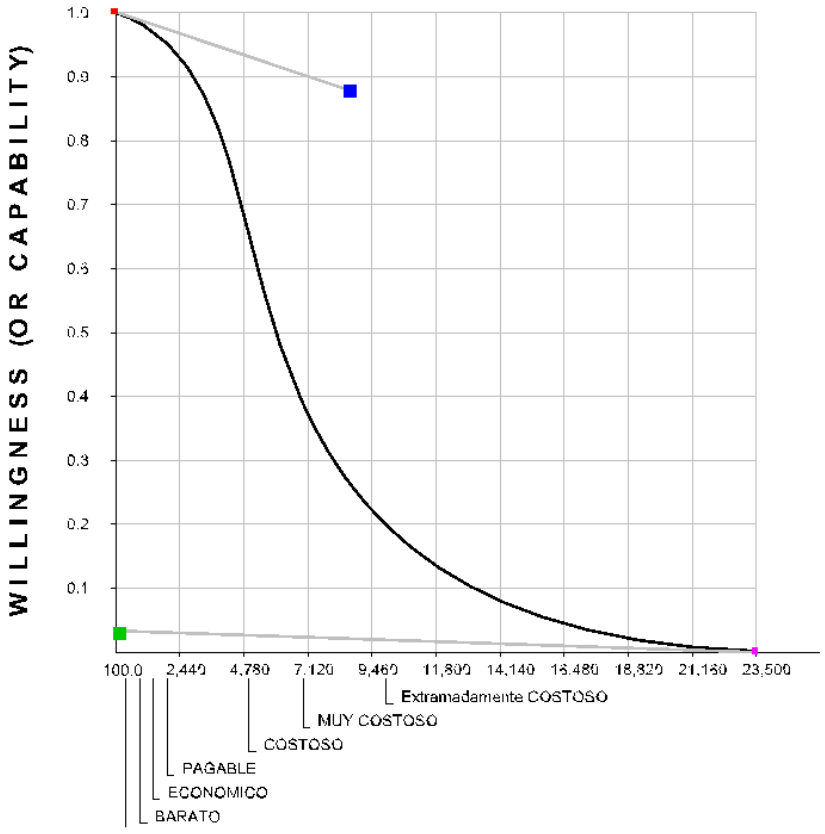



*Figura 20 Perfil de atacante basado en Valor del ataque (Amateur). Elaboración propia. @SecurITree V 5.2*

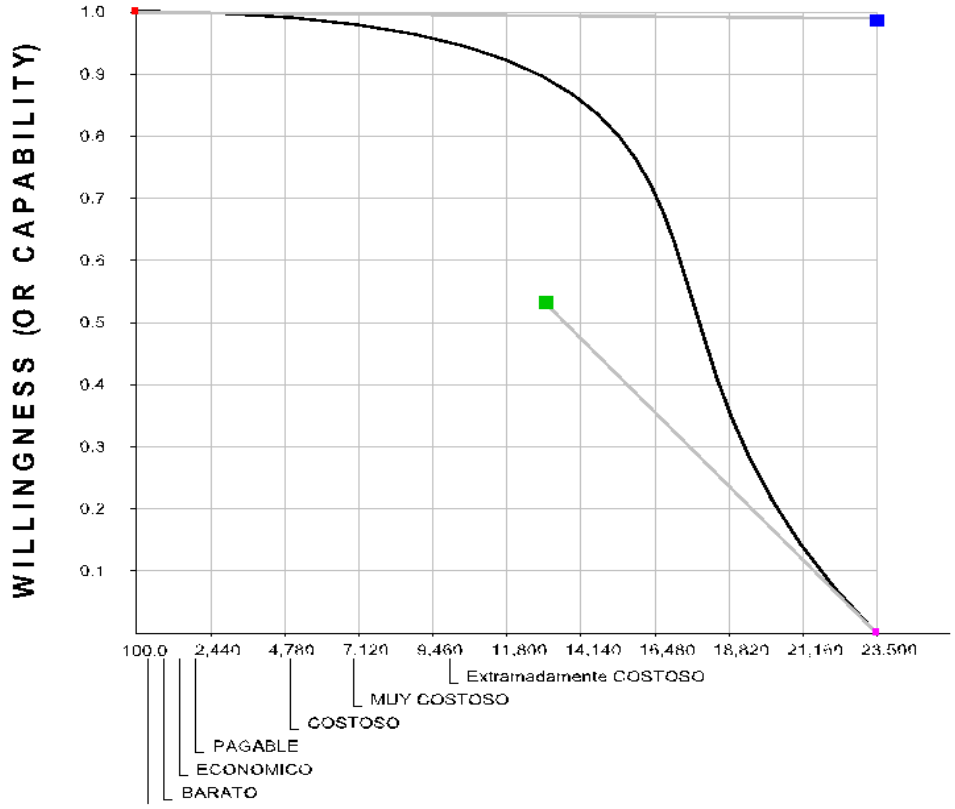



*Figura 21 Perfil de atacante basado en Valor del ataque (Profesional). Elaboración propia. @SecurITree V 5.2*

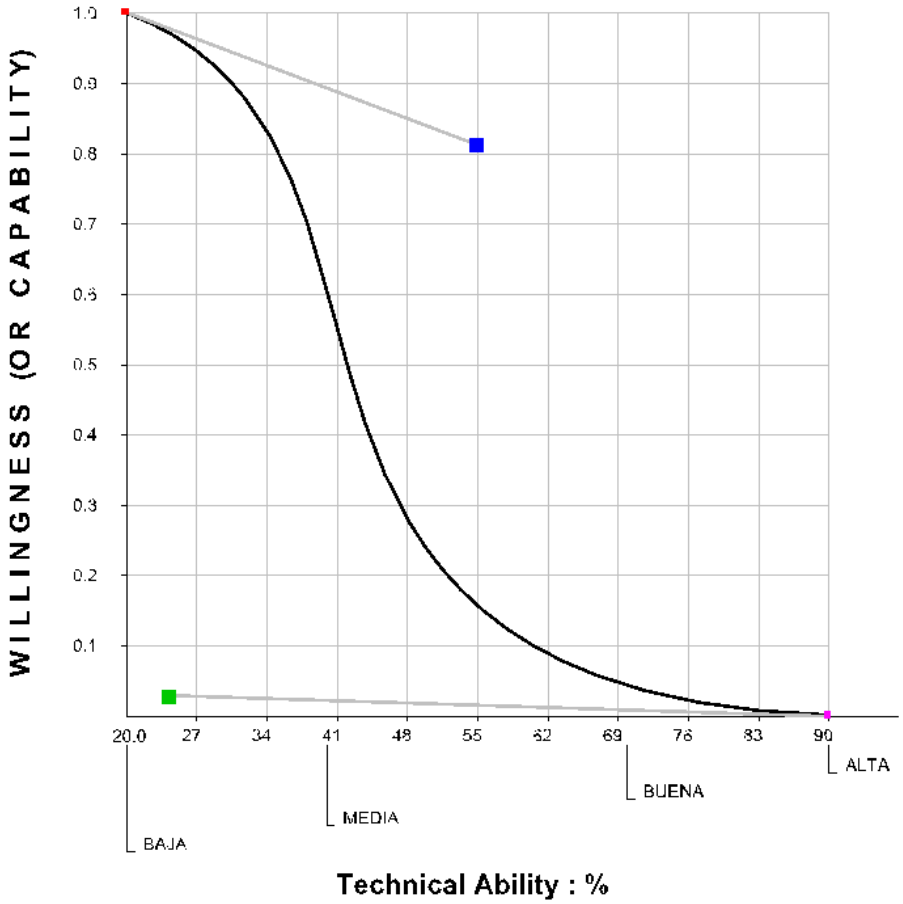



*Figura 22 Perfil de Atacante basado en su habilidad técnica (Amateur). Elaboración propia. @SecurITree V 5.2*

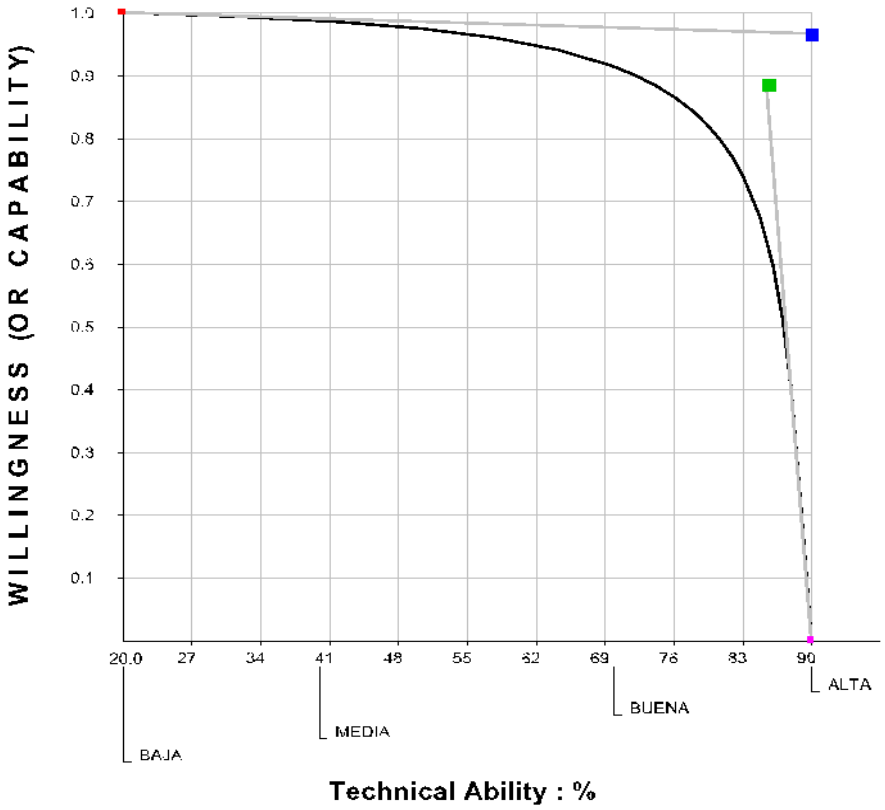



*Figura 23 Perfil de Atacante basado en su habilidad técnica (Profesional). Elaboración propia. @SecurITree V 5.2*

El mecanismo de poda simple descrito anteriormente proporcionó una representación cruda de la afinidad de los agentes de amenaza a sus recursos. Por ejemplo, suponga que el analista creó un perfil del agente de amenaza de un HACKER AFICIONADO (delincuente juvenil) que especificó un límite financiero de $10.000. Este perfil simplista afirma que el hacker aficionado está completamente e igualmente dispuesto a gastar cualquier suma entre $0 y $10.000, pero que serían totalmente incapaces o no estarían dispuestos a gastar $10.100.

Si bien no tenemos conocimiento de ninguna investigación sobre los hábitos de gasto de los delincuentes juveniles (Amateurs) que respaldarían la curva exacta que se muestra en la Figura 20, es más plausible que la Figura 22. La economía básica dicta que hay una escasez en casi todos los activos, y la renuencia correspondiente a gastarlo todo. Encontramos numerosos ejemplos donde la disposición de las personas a gastar disminuye gradualmente (y monótonamente), pero muy pocas situaciones donde la disposición es binaria.

Llamamos las funciones de utilidad a las funciones que mapean el apego de un atacante a las cantidades de los productos necesarios para realizar un ataque a un valor entre CERO y UNO. El dominio (valor del eje x) de estas funciones es el recurso bajo consideración. Por conveniencia, establecemos la convención de que el rango (salida) de las funciones será de 0 a 1 (Eje de las y). En general, las personas siempre están dispuestas a gastar nada de los recursos para adquirir una mercancía deseable. Esto se muestra en la Figura 20 por el punto de intersección con el eje y (0.1) en el gráfico. Nadie puede gastar más de lo que posee (no importa cuán atractivo sea el objetivo). El límite de su recurso es la intersección con el eje x.

Según la información que el analista tenga del atacante, se definen las funciones de utilidad de las variables de comportamiento que queremos modelar; Dependiendo del atacante, pueden valorar un recurso más que otro. El modelo puede reflejar el énfasis diferente que el atacante pone en diferentes recursos ajustando las formas de las curvas de utilidad. Por ejemplo, considere las funciones de utilidad del delincuente Amateur para el costo del ataque, la capacidad técnica. Ver figuras 20 y 22. De la Figura 20 vemos que la voluntad para realizar un ataque del Hacker aficionado, decrece exponencialmente si el costo del ataque está por encima de USD 5.000. De la Figura 22, podemos deducir que la voluntad para hacer el ataque de un Hacker aficionado decrece exponencialmente si se requiere buenas habilidades técnicas para lograrlo. Mientras las curvas de

utilidad, para un hacker profesional son bastantes diferentes. Su voluntad para realizar el ataque decrece exponencialmente si el costo para realizar el ataque es mayor a 15.000 y la habilidad técnica requerida es muy alta. Ver Figuras 21 y 23

Según TERRY 2021, existen varias alternativas para calcular la facilidad del ataque combinando las variables de comportamiento: Una alternativa es usar una suma ponderada. Por ejemplo, si existen tres indicadores de comportamiento, y el resultado de las funciones de utilidad para cada indicador son A, B y C, entonces podríamos calcular un valor general como

$$aA + bB + cC + \cdots + nN = Facilidad\ general$$

donde a + b + c = 1

El problema con este enfoque es que no refleja el hecho de que la falta de un solo recurso es suficiente para evitar que un adversario realice un ataque.

Un problema con el uso de un producto simple es que el valor de Facilidad de ataque tiende a disminuir a medida que se agregan indicadores adicionales al modelo. Este efecto puede compensarse tomando la raíz enésima del producto, es decir, la media geométrica.

Por lo tanto, la decisión del atacante está limitada por la lógica del nodo AND. (Media geométrica de sus componentes)

*Facilidad de ataque = Función de utilidad1 (variable comportamiento 1) * función de utilidad 2 (variable de comportamiento 2) * función de utilidad 3 (variable comportamiento 3) … función de utilidad N.*

Es importante resaltar que la curva de función de utilidad que mapea el valor monetario ($) en un rango de cero a 1, pretende describir la percepción de valor de ese activo para el atacante.

Dado que el resultado de este cálculo depende en gran medida de las funciones de utilidad, es justo preguntar cómo se derivan. La forma de la curva se basa en varios supuestos. Creemos que las personas están completamente dispuestas cuando no tienen que consumir recursos (económicos, técnicos). Por lo tanto, para x = 0 podemos afirmar con seguridad que y = 1. Aunque estrictamente hablando, esto es una suposición, es una fundamentación bien fundada. Las personas están muy inclinadas a perseguir los objetivos que desean si son gratis.

También sabemos que la voluntad (y la capacidad) de gastar del atacante llegará a cero cuando la cantidad de recursos sea igual o superior a la cantidad que controlan. Esto significa que la curva cruza el eje horizontal en el límite del recurso del agente de amenaza (atacante). La precisión de esta suposición dependerá de la calidad de la inteligencia que tengamos sobre los recursos de nuestro adversario. Generalmente conocemos a nuestro adversario lo suficientemente bien como para estimar el presupuesto de recursos de él al menos en el orden de magnitud correcto.

Para determinar la forma de la curva entre los dos puntos finales, sería ideal si pudiéramos hacer referencia a estudios psiquiátricos exhaustivos sobre la psique de una amplia variedad de adversarios. Desafortunadamente, esa base de información no existe. Se requiere otra estrategia para seleccionar la forma de la curva.

Se podría usar una línea recta simple para unir los dos puntos finales conocidos. Eso, al menos, transmite la premisa de que el adversario tiene una menor voluntad de desprenderse del recurso a medida que aumenta la cantidad a gastar. Sin embargo, es posible realizar más ajustes si consideramos la psicología del adversario.

Un adversario audaz (Figura 21) que es fácilmente persuadido para gastar sus recursos puede ser representado usando una curva convexa (al mirar desde arriba). Su disposición a gastar

no disminuye hasta que casi llegan al límite de sus recursos. Por otro lado, un adversario tímido (Figura 20), que está fuertemente apegado a un recurso, será reacio a gastarlo. Esto produce una curva cóncava (al mirar desde arriba).

Debido a las variaciones en el comportamiento humano dentro de una clase de agente de amenaza, ninguna curva será una descripción perfectamente precisa del proceso de toma de decisiones de un agente de amenaza específico. Si bien reconocemos las limitaciones inherentes a este método de cálculo de la Facilidad de ataque, creemos que puede ser una representación útil de la facilidad de un ataque tal como lo percibe el adversario.

A veces es conveniente hablar de Dificultad de ataque (como lo opuesto a Facilidad de ataque). Los dos términos son (no filosóficamente, si no matemáticamente) el inverso el uno del otro:

$$Dificultad\ de\ ataque = \frac{1}{Facilidad\ de\ ataque}$$

Calcular la facilidad de un ataque es solo parte de la ecuación, ya que necesitamos combinarla con la motivación del atacante, es decir la propensión de un ataque es el resultado medir la facilidad del ataque y (AND) los beneficios que el atacante tenga, es decir de la motivación.

3.5.1.2. Motivación del atacante.

Las motivaciones del atacante están directamente relacionadas con los beneficios del Ataque. Anteriormente se afirmó que los adversarios toman decisiones basados en el costo-beneficio. El cálculo del valor de Facilidad de ataque consideró los costos del escenario de ataque,

pero no sopesó los beneficios que el atacante esperaba obtener de un escenario de ataque. También deben tenerse en cuenta para comprender qué tan atractivo le parece un ataque a un adversario.

En el ejemplo de un ataque de denegación de servicios, discutido anteriormente, los beneficios del atacante podrían ser principalmente monetarios.

Según Terry (2021), en situaciones más complejas, se pueden obtener múltiples tipos de beneficios al llevar a cabo escenarios de ataque. Los adversarios se sentirán atraídos por escenarios específicos dependiendo de la combinación particular de recompensas. Diferentes escenarios proporcionarán diferentes niveles de motivación del atacante.

Toda la interacción directa entre un adversario y su objetivo se captura en los nodos hoja del árbol de ataque. Sin embargo, muchos (y generalmente la mayoría) de los beneficios que un adversario obtiene de un ataque están asociados con estados lógicos más altos en el árbol. Por lo general, los mayores beneficios del atacante están asociados con el nodo raíz del árbol, adicional a los beneficios secundarios que se producen en los diversos nodos intermedios. Dado que los diferentes escenarios de ataque atraviesan diferentes caminos entre los nodos hoja y la raíz, los beneficios del atacante pueden diferir considerablemente dependiendo del escenario de ataque utilizado.

La mayoría de los tipos de recompensas exhiben una utilidad decreciente. Incluso el dinero pierde su impacto después de cierto punto.

¡No tiene sentido tener juguetes si estás demasiado ocupado trabajando para jugar con ellos!

El atractivo de una recompensa dada es subjetivo. Un delincuente juvenil (Hacker Aficionado) con un trabajo de salario mínimo (o ninguno) puede ver $50,000 como riqueza ilimitada. El beneficio decreciente de la riqueza para un delincuente Amateur se muestra en la

Figura 24. El beneficio es una medida del valor percibido de un recurso particular. Las funciones que asignan a las cantidades absolutas del recurso al valor percibido se denominan funciones de utilidad de beneficio del atacante.

Los atacantes toman sus decisiones en función de sus percepciones de los resultados de un curso de acción particular. De hecho, pueden estar equivocados en su estimación. En este caso, la percepción es mucho más importante que la realidad.

Así como los impactos predominantes en las víctimas tienden a ocurrir en niveles más altos en el árbol, también lo hacen muchos de los beneficios de los atacantes.

Usando las funciones de utilidad mostradas, se obtiene que:

$F_{\text{costo amateur}}(4780) = 0.7$

$F_{\text{habilidad técnica amateur}}(41) = 0.54$

Por lo tanto, $Facilidad\ de\ ataque = 0.7 \times\ 0.54 = 0.378$

$F_{\text{costo profesional}}(4780) = 0.99$

$F_{\text{habilidad técnica profesional}}(40) = 0.98$

Por lo tanto, $Facilidad\ de\ ataque = 0.97$

De este análisis simple, se puede verificar que un ataque denegación de servicios, cuyo atacante consume la misma cantidad de recursos (técnicos y económicos), es mucho más factible para un hacker profesional que un atacante Junior, debido a que sus curvas que describen su comportamiento son diferentes.

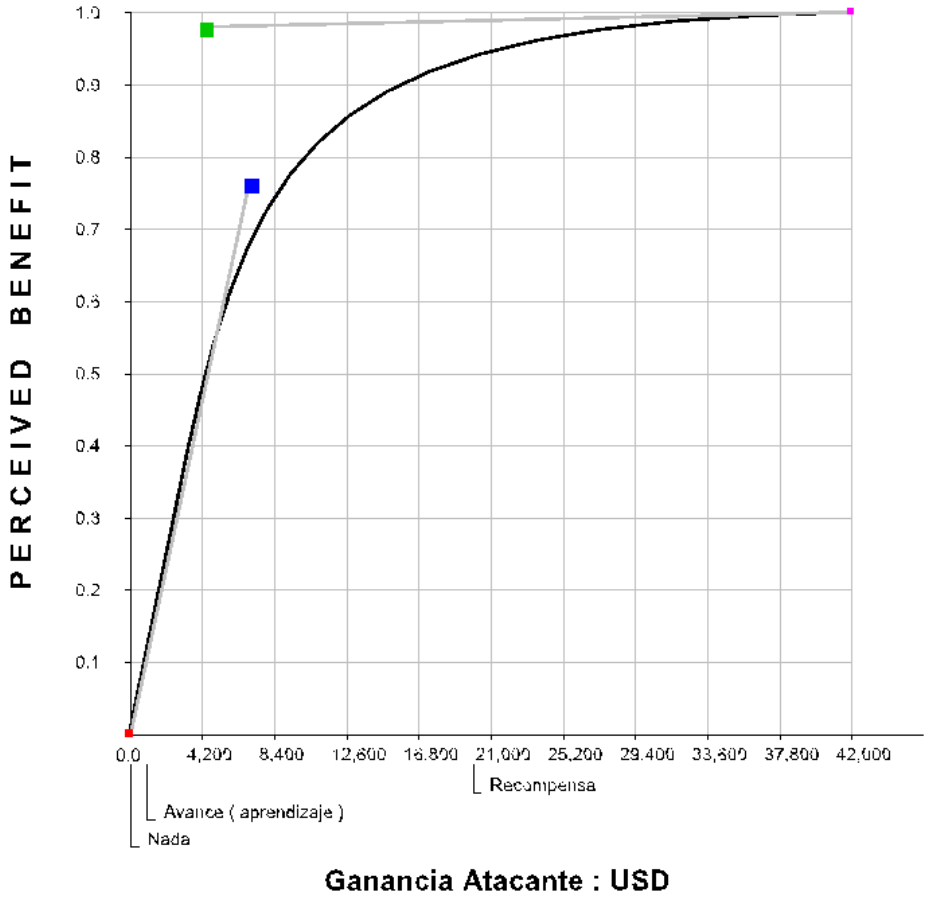



*Figura 24 Motivación Hacker Amateur por Cantidades Crecientes de Dinero. Elaboración propia. @SecurITree V 5.2*

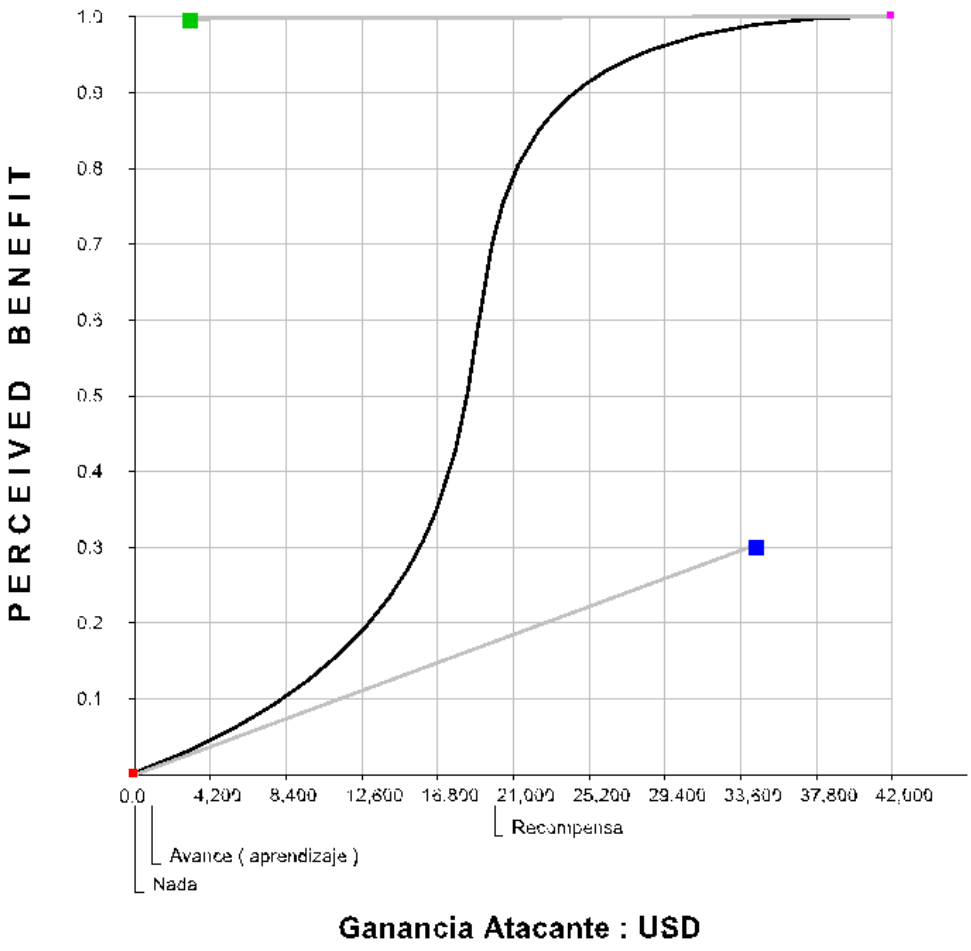



*Figura 25 Motivación del Hacker Profesional por Cantidades Crecientes de Dinero. Elaboración propia. @SecurITree V 5.2*

Ahora, para completar el cálculo de la probabilidad de un ataque, falta incluir en el análisis cuales serían los beneficios del atacante. Un Hacker Profesional podría tener aspiraciones mucho más altas que el delincuente juvenil (Hacker Amateur) Incluso pueden sentir que, por debajo de un cierto umbral, una actividad en particular no vale la pena. La curva de beneficio del atacante para esa persona se ve en la Figura 24. La cual muestra que el Hacker Profesional no tiene mucha

motivación para hacer nada ilícito hasta que la recompensa llegue a alrededor de $12.000. Por encima de $12.000, el deseo aumenta rápidamente hasta alrededor de $25.000(en ese momento la codicia del Hacker Profesional se está saciando). Mientras para un Hacker Amateur, cuya curva de beneficio se puede observar en Figura 25, estara muy motivado con ganancias superior a $5.000.

Las curvas de beneficios son ajustables dentro de las herramientas de modelamiento de Árboles de ataque, por el analista que está realizando el modelo, con base el conocimiento que vaya adquiriendo del comportamiento del atacante. Este trabajo de investigación utilizo la herramienta *SecurITree @Amenaza.*

Como se mencionó anteriormente, el dinero es solo uno de los varios beneficios posibles que se pueden obtener a través de un ataque. La venganza, el prestigio, el poder y las diversas gratificaciones de los deseos son todas posibilidades. Estos podrían representarse a través de otras funciones específicas del agente de amenaza (todas las cuales también generarían valores entre 0 y 1).

Según Terry 2021, Cuando existen múltiples recompensas, es necesario combinar la salida de las funciones de utilidad de beneficio del atacante correspondiente. La técnica de multiplicación utilizada anteriormente para combinar las funciones de facilidad de ataque no funciona bien para combinar las funciones de utilidad de beneficio del atacante. Si se usa la multiplicación, solo se puede obtener una puntuación alta si el ataque beneficia al atacante de todas las formas mensurables. Esto no es realista. Incluso si un ataque no proporciona todos los beneficios imaginables, un atacante aún puede encontrar un subconjunto de recompensas potenciales muy atractivo. Por esa razón, es preferible usar una suma ponderada para evaluar el valor combinado de las funciones de utilidad de beneficio del atacante.

$$aA + bB + cC + \cdots + nN = Beneficios\ obtenidos\ (Deseabilidad)$$

donde a + b + c = 1

Sería simplista creer que los ataques exitosos solo traen beneficios positivos a un atacante. Además del uso de recursos, un ataque puede tener uno o más efectos perjudiciales para el atacante

El atacante podría enfrentar tiempo en la cárcel, lesiones o incluso la muerte por llevar a cabo el ataque. Al aplicar una técnica similar a la utilizada para los beneficios del atacante, es posible calcular una suma ponderada de las desventajas del atacante. Si la suma de los beneficios y las desventajas del atacante es positiva, significa que la percepción general del ataque del adversario es favorable y éste estará motivado para intentarlo (dentro de sus limitaciones de recursos). Si la suma es negativa, significa que las desventajas superan los beneficios y que el atacante rechaza los intentos de ataque de esa naturaleza. Para simplificar las discusiones, generalmente hablaremos solo de los beneficios del atacante de un escenario de ataque, pero siempre debe recordarse que esto realmente abarca tanto los beneficios como las desventajas.

Anteriormente afirmamos que los atacantes tienen más probabilidades de realizar ataques que proporcionan un alto rendimiento con un bajo gasto de recursos.

Dado que

$$\boldsymbol{Dificultad\ de\ ataque\ (costo\ de\ ataque\ percibido) = \frac{1}{Facilidad\ de\ ataque}}$$

y que los atacantes seleccionarán ataques en función de su conveniencia, esto significa que la PROBABILIDAD DE UN ATAQUE lo podemos aproximar a:

$$\boldsymbol{Propensidad\ de\ ataque = Facilidad\ de\ ataque \times\ Beneficio\ del\ ataque}$$

### 3.5.4. **Cálculo del impacto.**

La percepción de dolor de una víctima, para un mismo ataque, cambia de una víctima a otra. la cual debemos cuantificar con una curva de percepción de la utilidad donde en el eje de la X esta la cantidad de dolor y en el eje de las Y esta la normalización de la percepción de dolor, donde 0 significa ningún dolor y 1 significa mucho dolor, quizás irresistible. La curva de dolor debe reflejar el impacto que tiene para los directivos que una amenaza de un ataque se concrete. Por ejemplo, para universidad "pública" estar fuera de servicio 4 horas, debido a un ataque DDoS, puede significar un dolor mínimo, (0.1) ver Figura 23, dicho ataque para una Habilidad víctima 2 (universidad privada) puede significar un gran dolor (0,7), ver Figura 24.

Es muy importante, poder determinar la curva de percepción del dolor de la víctima, ya que los recursos económicos asociados a las inversiones en ciberseguridad estarán impactados por la percepción del dolor de la víctima. En otras palabras, las inversiones en seguridad están relacionadas con la tolerancia al riesgo del decisor. Una organización con alta tolerancia al riesgo puede soportar ataques DDoS que lo dejen fuera de servicio 4 horas, mientras para otras organizaciones estar por fuera de servicio una hora puede considerarse un desastre.

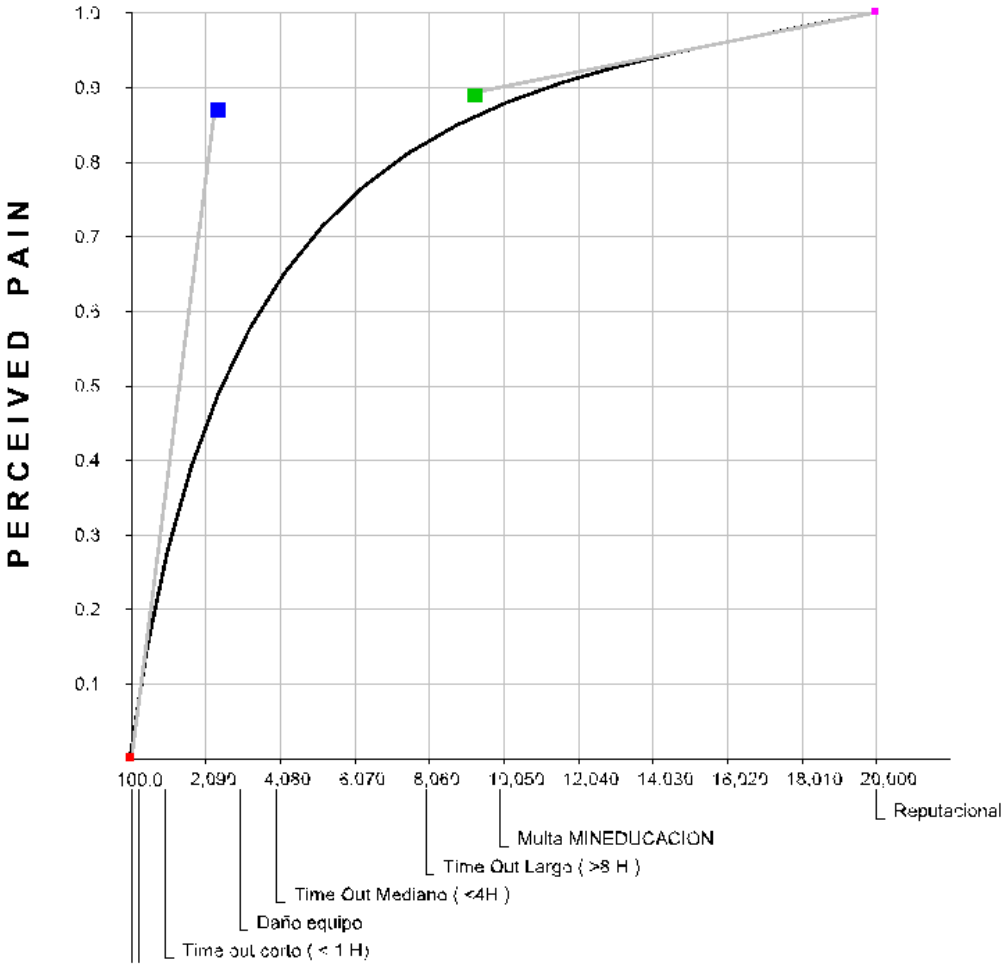



*Figura 26 Comportamiento del dolor percibido por el ataque DDoS para una victima1 (institución privada). Elaboración propia. @SecurITree V 5.2*

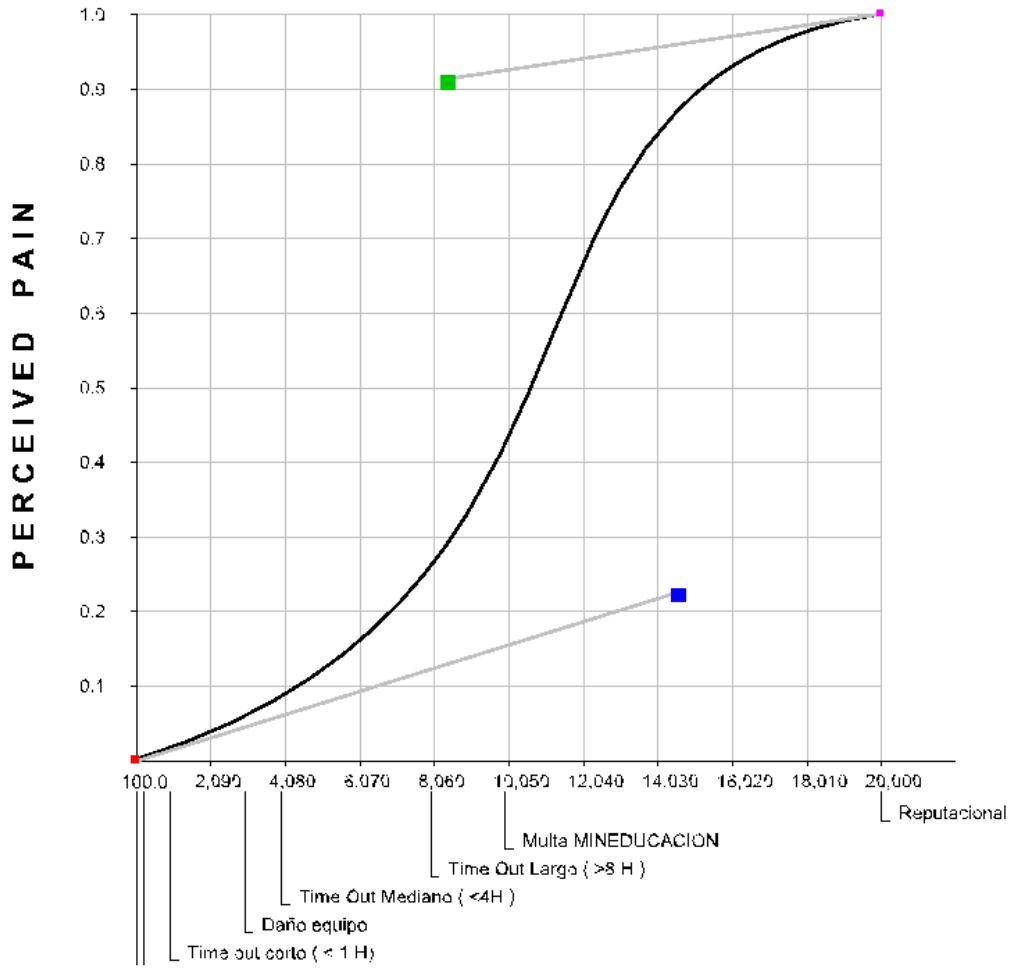



*Figura 27 Comportamiento del dolor percibido por el ataque DDoS para una victima1 (institución pública). Elaboración propia. @SecurITree V 5.2*

Una vez calculada la probabilidad y el impacto de un ataque podemos calcular el Riesgo de un ataque, por ejemplo, Riesgo de un ataque de Denengacion de Servicios.

Recordemos un poco, porque llegamos aquí a estas ecuaciones. Todo inicia cuando queremos calcular el Riesgo Mitigado de una Contra- Medida.

$$\boldsymbol{RIESGO = PROBABILIDAD\ DEL\ ATAQUE\ x\ IMPACTO}$$

La probabilidad podemos equiparla a la que tan propensos somos a un ataque.

| FACILIDAD PARA REALIZAR UN ATAQUE DDoS | | | | | |
|---|---|---|---|---|---|
| | | AMATEUR | | PROFESIONAL | |
| | | COSTO ABSOLUTO | FACILIDAD DEL HACKER Normalizado | COSTO ABSOLUTO | FACILIDAD DEL HACKER. Normalizado |
| COSTO DEL ATACANTE | COSTO DEL ATAQUE | 4.780 | 0.7 | 4800 | 0.99 |
| | HABILIDAD TÉCNICA | Media (40%) | 0.54 | Media (40%) | 0.98 |
| | | FACILIDAD GENERAL | 0.378 | FACILIDAD GENERAL | 0.97 |

*Tabla 3. ESTIMACION DE FACTIBILIDAD PARA REALIZAR UN ATAQUE ddos. Elaboración propia.*

El riesgo de un ataque de DDoS, cambia dependiendo del perfil de la víctima y del atacante, así:

Dado esto podemos deducir que:

$$Riesgo = Probabilidad\ x\ Impacto$$

Riesgo $_{\text{u pública amateur}}$ = 0.378 x 0.1 = 0,0378

Riesgo $_{\text{u pública profesional}}$ = 0.97 x 0,1 = 0,097

Riesgo $_{\text{u privada amateur}}$ = 0.378 x 0.7= 0.2646

Riesgo $_{\text{u privada profesional}}$ = 0.97 x 0.7 = 0,679

Como se puede observar en la FIGURA 27, el Riesgo de que se materialice una amenaza depende de los recursos del atacante (tanto técnicos como económicos), los beneficios que reciba el atacante y de la percepción del dolor que dicho ataque produzca en la victima. Para una Víctima 2 que es bastante sensible al dolor del ataque, tiene un Riesgo más alto de que se materialice un ataque. Ver figura 28.

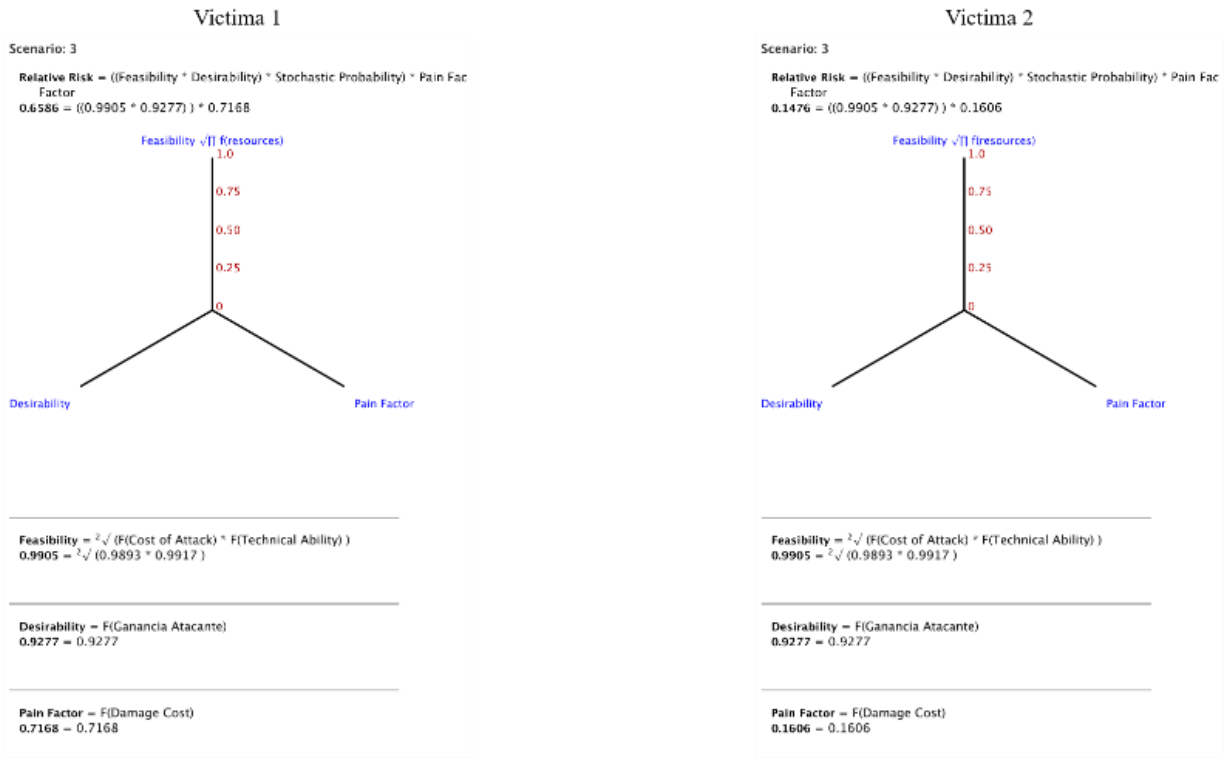



*Figura 28 Factores que influyen en el cálculo del Riesgo, para 2 víctimas con diferente tolerancia al riesgo. Elaboración propia. @SecurITree V 5.2*

Al ver la figura 28 podemos comprobar que, para un mismo escenario de ataque, donde suponemos el mismo perfil de atacante en ambos casos, el Riesgo calculado por las dos víctimas es diferente; ya que, para la victima 1 (Figura 26), estar por fuera de servicio 8 horas, lo percibe como un dolor de 0,71, en la escala de 0 – 1; donde CERO significa que no te duele y UNO

significa que el impacto es catastrófico. Mientras para la victima 2 (Figura 27), la misma indisponibilidad del servicio (8 Horas) lo percibe como un dolor de 0,16. Es decir las dos víctimas valoran el riesgo del mismo escenario de ataque, en forma diferente; por lo tanto, el dinero que estarían dispuestos a invertir en ciberseguridad esta correlacionado con dicha valoración del riesgo.

### 3.6 Descripción del proceso de análisis económico de inversiones usando Árboles de ataque

A continuación, vamos a colocar en práctica toda la teoría expuesta anteriormente para calcular cuánto dinero disponible hay para diferentes contramedidas, en dos diferentes instituciones, cada una de ellas con una tolerancia al riesgo diferente.

Para dicha victima debemos hacer la evaluación económica de las contramedidas que disminuya el riesgo de un ataque de DDoS, se propone diagrama de flujo.

1. Debemos construir el árbol para un ataque especifico (descripción cualitativa de los diferentes escenarios o alternativas de cómo se podría llevar a cabo el ataque:
2. Debemos incluir los posibles costos que dicho ataque implica y construir las funciones de percepción de valor de dichos costos para determinado perfil de atacante. (función de utilidad de los costos)
3. Con base en estos dos análisis calculamos que tan fácil es el ataque.
4. Debemos extrapolar los posibles beneficios que el atacante logra con el éxito de dicho ataque. Con base en eso se construye las curvas de percepción de valor de esos beneficios para cada atacante (función de utilidad de deseabilidad).
5. Una vez calculado la facilidad del ataque y la deseabilidad del ataque calculamos, que tan expuestos estamos un ataque. Es decir, que probabilidad tenemos de que dicho ataque se lleve a cabo.

6. Calculamos el impacto en la victima que dicho ataque produciría, construimos la curva de percepción de valor del impacto, según el perfil de la víctima.
7. Teniendo en cuanta la probabilidad de ocurrencia del ataque y el impacto que dicho ataque tiene, calculamos las expectativas de perdida (Loss Expectancy) en un periodo de tiempo, por ejemplo, en un año (Anual loss expetanncy: ALE).
8. Todo este cálculo se hace para el árbol de ataque básico (sin contramedidas) y después para cada contramedida. de esta forma calculamos como se reduce el riesgo una vez se adopte una contramedida.

### 3.6.1 Caso de uso.

Priorizaciones de inversiones para disminuir el riesgo de un ataque de denegación de servicios DDoS, por sus siglas en inglés (Distributed Denial of services).

Es importante recordar la metodología propuesta para priorizar las inversiones en ciberseguridad, usando Árboles de Ataque. Es una metodología que mezcla una análisis cualitativo y cuantitativo. Tal como se muestra en la Figura 29, para poder calcular el ROSI de una medida de ciberseguridad usando Árboles de ataque debemos antes seguir los siguientes pasos:

1. Construir el Perfil de la víctima y del atacante.
2. Construir el Árbol de ataque Base que describe un ataque DDoS
3. Calcular el Riesgo, probabilidad de ataque, ALE, Impacto y Riesgo de cada escenario de un posible ataque del árbol base.
4. Incluir una contramedida y volver a calcular el ALE, el riesgo residual que dicha contramedida introduce en los diferentes escenarios donde aplica.

5. Con el ALE base y el riesgo mitigado (delta entre el riesgo base y el riesgo residual que la contramedida impacta) se calculan las diferentes cantidades de dinero que la administración está dispuesta a invertir para que dicha medida tenga ROSI positivo.
6. Se ordenan de mayor a menor las contramedidas, teniendo en cuenta el valor de dinero que está disponible para invertir.
7. Esto se repite el proceso para una segunda víctima con una tolerancia al riesgo diferente del caso inicial.
8. Se compara la disponibilidad de dinero a invertir en ciberseguridad dependiendo del perfil de riesgo.

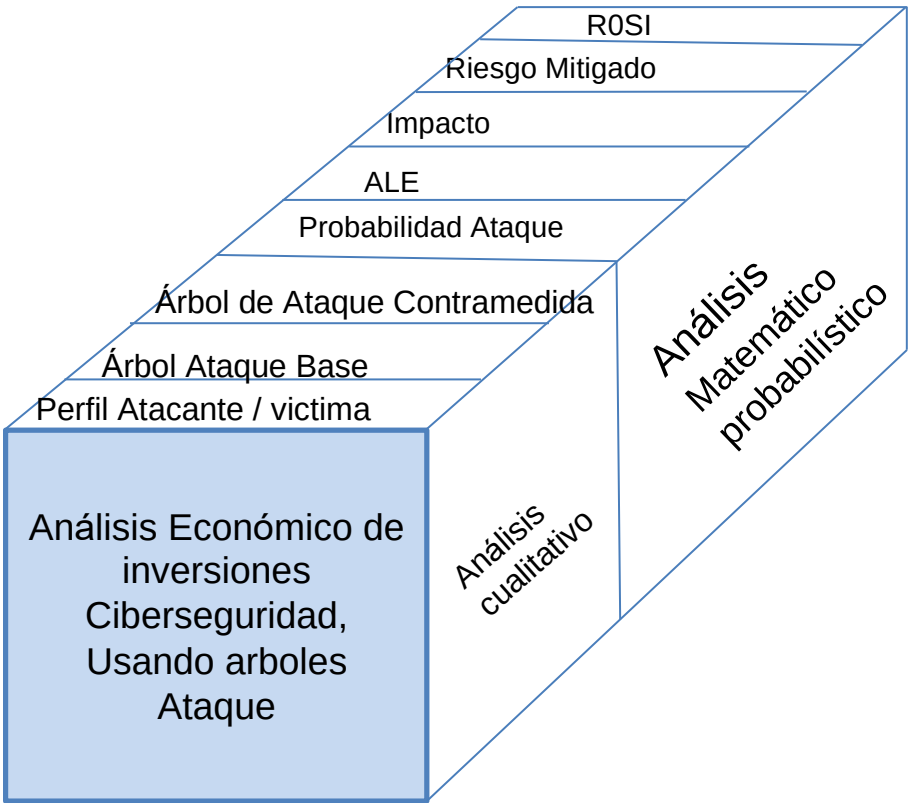



*Figura 29 Descripción metodológica de cálculo del ROSI – Usando Árboles de Ataque. Elaboración propia.*

**Descripción Ataque DDoS.**

Un ataque de denegación de servicio se caracteriza por un intento explícito de los atacantes de impedir el uso legítimo de un recurso / servicio. Un ataque distribuido de denegación de servicio implementa varias máquinas atacantes para lograr este objetivo.

Hay muchas formas de perpetrar un ataque de denegación de servicio; según Mircovic & Reiher (2004) se pueden clasificar en las siguientes categorías:

- Volumétricos: Intenta consumir el ancho de banda de la red objetivo. Este ataque pretende elevar el nivel de congestión de la red.
- Ataques Basados en TCP: Un atacante intenta consumir las tablas de estado de la conexión que están presente en muchos componentes de la infraestructura de la victima
- Ataques de capa de Aplicación: En ataques a la capa de aplicación, un atacante intenta explotar algunas de las debilidades en los protocolos de capa de aplicación tales como HTTP, SMTP, DNS, y SIP / VoIP, etc. Estos ataques de capa 7 son muy peligrosos, ya que son difíciles de detectar. Ataques simples de inundación a la capa de aplicación tales como HTTP GET inundación, inundación HTTP POST, etc. han sido uno de los ataques DDoS más comunes.

Según KARPESKY (2020) muestra que, en los últimos años los tipos y tamaños de organizaciones en el punto de mira se ampliaron sustancialmente. En el primer trimestre de 2020 observamos un aumento significativo tanto en el número de ataques DDoS como en su calidad. En comparación con Q4 2019, el número de ataques se duplicó y, en comparación con el primer trimestre de 2019, creció en un 80%. Además, los ataques se hicieron más largos: observamos un claro aumento tanto en el promedio como en el máximo de la duración de los ataques.

Podría haber ciertas razones para este aumento sustancial de los ataques, pero la más importante, la accesibilidad de las herramientas y técnicas que se utilizan para realizar ataques DDoS. Las redes de bots pueden ser contratados en calidad de alquiler para realizar ataques DDoS. Hay *masters* botnet ofreciendo una botnet (12k) en alquiler - por el precio de 500$ por mes, según los estudios de ALQUILER DE BOTS (s.f) y el informe McAfee Ciberguerra. (s.f)

Antes empezar a construir el árbol de ataque que describe un ataque de denegación de servicio es importante caracterizar el tipo de amenaza, tal como se describió en el capítulo 1.

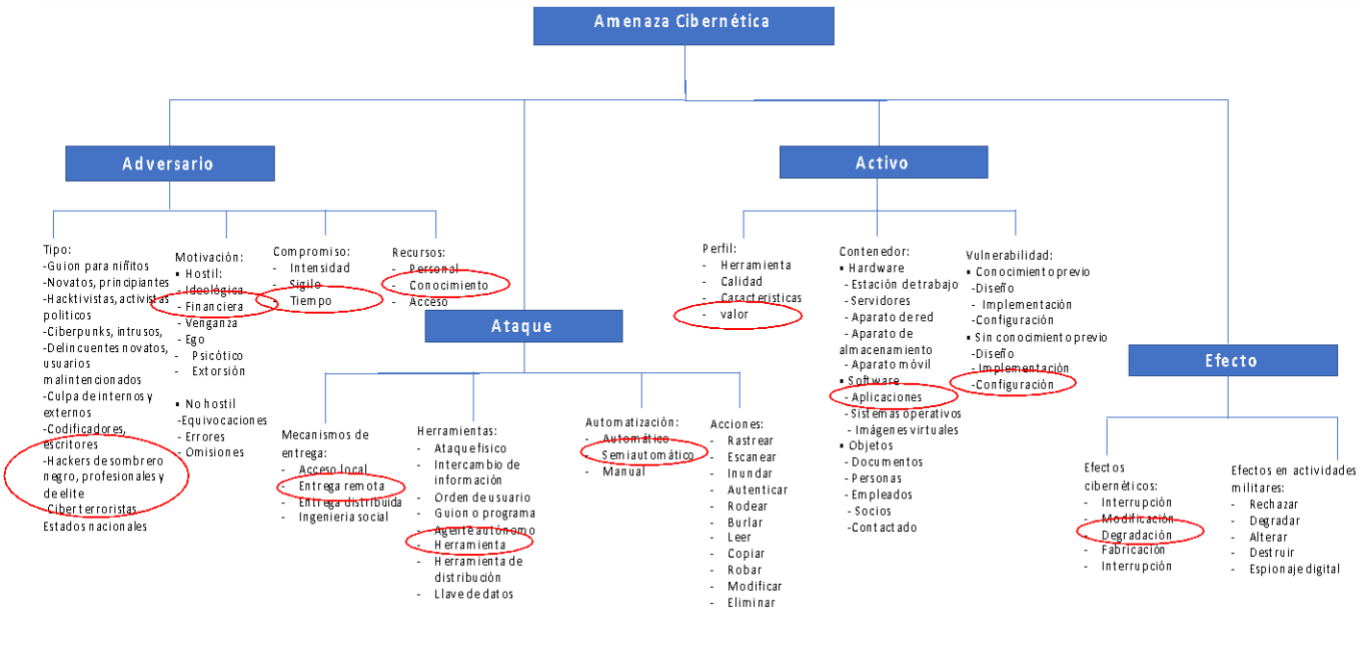



*Figura 30. Caracterización de un ataque de DDoS. Elaboración propia.*

Podemos describir que el atacante al cual nos enfrentamos es un Hacker profesional, que tiene una motivación financiera, tiene un conocimiento y planeara el ataque son afanes y con mucho sigilo. El Ataque sobre la disponibilidad del servicio de más alto impacto será un ataque remoto, usando herramientas especializadas, semiautomático. El activo para atacar será una aplicación de más uso por los clientes de una institución educativa: aplicación de carga de programa académico.

Para determinar el perfil de atacante con más precisión y saber cuántos recursos está dispuesto a invertir se debe hacer un ejercicio de perfilamiento con expertos en el tema. Para nuestro ejercicio hemos supuesto las siguientes curvas de comportamiento del atacante que hemos denominado un hacker profesional:

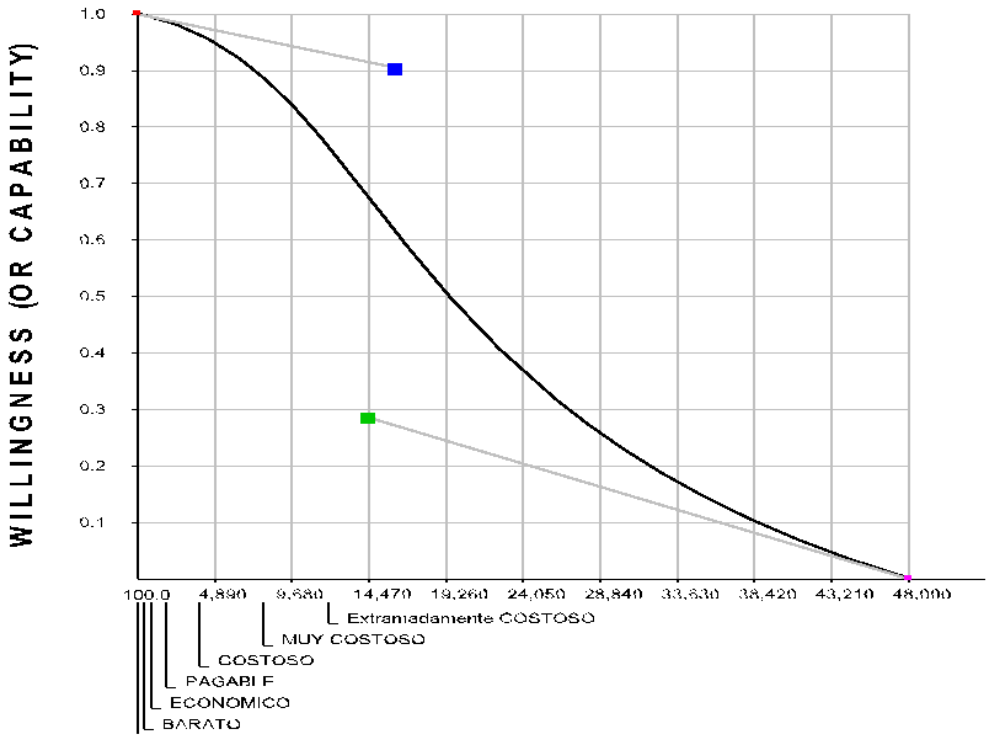



*Figura 31 Disposición a gastar dinero por parte del atacante. Elaboración propia. @SecurITree V 5.2.*

Esta grafica indica que su voluntad para realizar al ataque disminuye conforme el ataque le cuesta más, mientras el ataque le cueste menos de USD 14.000, él está dispuesto a realizar el ataque con una voluntad de 0,7.

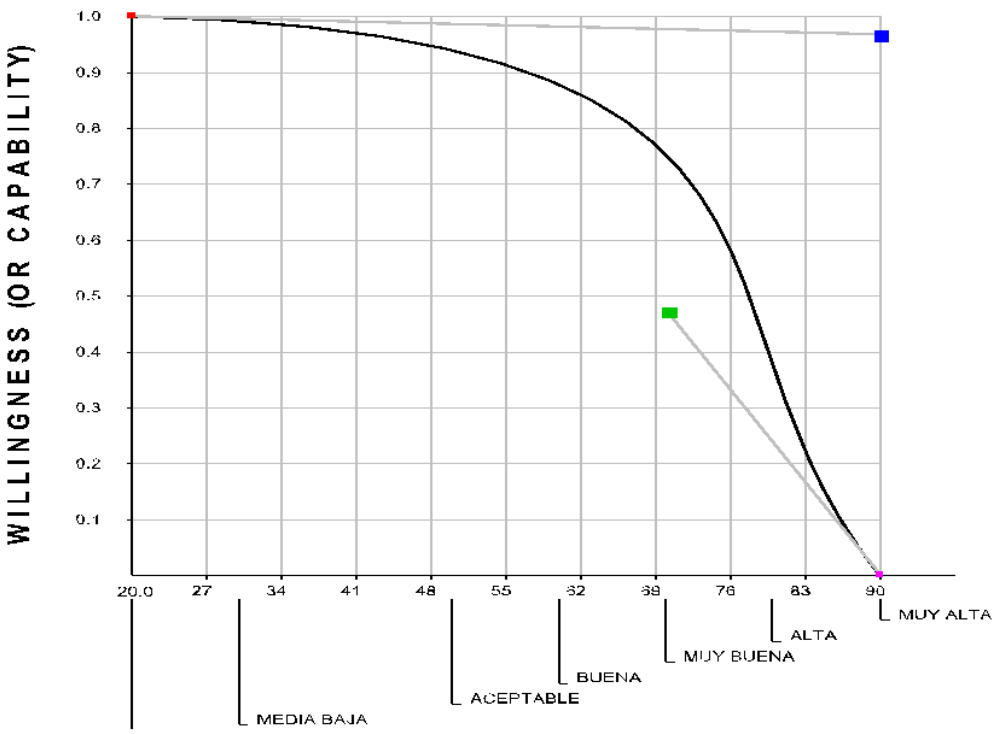



*Figura 32 Disposición de habilidad Técnica que está dispuesta a "gastar". Elaboración propia @SecurITree V5.2*

Esta grafica nos indica que este atacante mantiene una disponibilidad atacar hasta que la exigencia técnica para sobrepasar la contramedida sea **ALTA**. Si la vulnerabilidad de la víctima es muy obvia y requiere una habilidad técnica media aceptable o menor, su disposición atacar por este concepto es mayor 0,8.

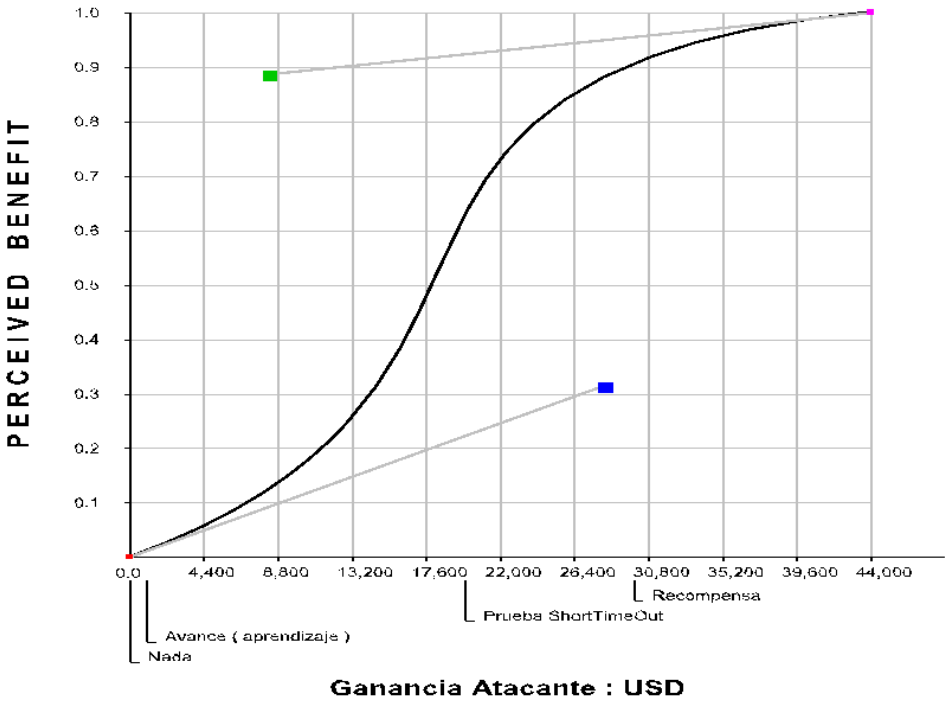



*Figura 33 Percepción de Valor del atacante Hacker Profesional. Elaboración propia. @SecurITree V 5.2*

Este atacante su interés a seguir ganando dinero después de los USD 30.000 USD, de crecer marginalmente. Si la recompensa a recibir por el ataque oscila entre 15.000 y 25.000, su interés se incrementa exponencialmente.

Aquí es importante recordar que la Probabilidad de un ataque se calcula de la siguiente forma:

**Prob ataque = Facilidad de ataque * Beneficio que recibe el atacante.**

La Facilidad de un ataque depende de los recursos técnicos y económicos que esta dispuestos a invertir el atacante. Todos los atacantes están dispuesta a realizar el ataque si no les cuesta nada (técnica ni económicamente), su disposición atacar va decreciendo conforme el costo se va incrementando, conforme a las curvas que identifican su comportamiento.

Para poder calcular el Riesgo, es importante perfilar la tolerancia al riesgo de la víctima. Es decir, debemos entender la percepción de dolor de la víctima ante un ataque especifico, para los cual debemos entrevistarnos con las directivas de la organización para saber lo que significa para ellos, está fuera de servicio por una hora, dos, tres, ocho o más horas. No tiene el mismo impacto económico, estar fuera de servicio 4 horas, para una tienda ON LINE que para una institución universitaria.

Para poder analizar cómo se comporta el riesgo antes diferentes perfiles víctima, se diagrama dos perfiles de víctima, con una percepción de dolor (tolerancia al riesgo) diferente.

Según la curva del dolor percibido, tenemos en el eje de las Y el dolor en una escala entre 0 y 1, donde 0 significa que no le duele nada y 1 que su dolor es máximo. En el eje de las X el impacto del ataque DDoS medido en valores absolutos, donde se le da un valor USD 1.000 aproximadamente por cada hora de falla de indisponibilidad del servicio por un ataque de DoDS. Estos son supuestos académicos, para validar la propuesta metodológica del trabajo de grado. En el mundo real se debe hacer las respetivas entrevistas para capturar esos perfiles de riesgo de la víctima.

Para una víctima con baja tolerancia al dolor (Victima Privada), podemos decir según la Figura 34. que una indisponibilidad del servicio de 4 horas le significa un dolor 0,6, mientras para otra víctima que hemos llamada Victima Pública, según la Figura 35., esa misma falla de indisponibilidad es percibido con un índice menor a 0,1, es decir no le genera mayor dolor.

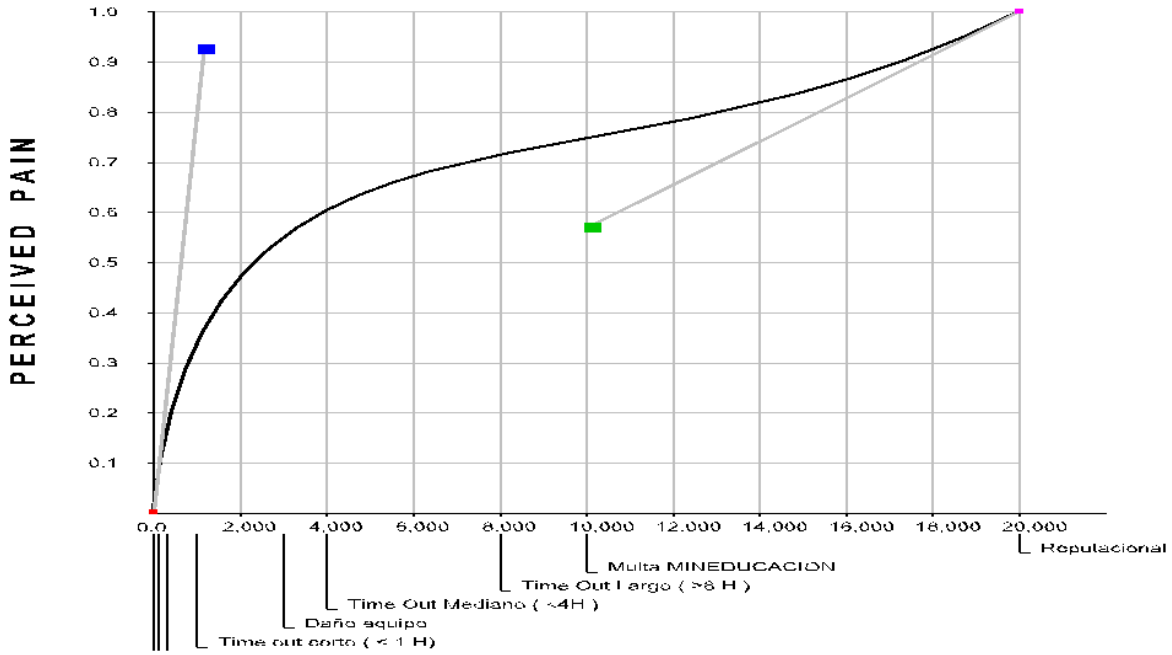



*Figura 34 Perfil victima Privada con Baja Tolerancia al Dolor. Elaboración propia. @SecurITree V 5.2*

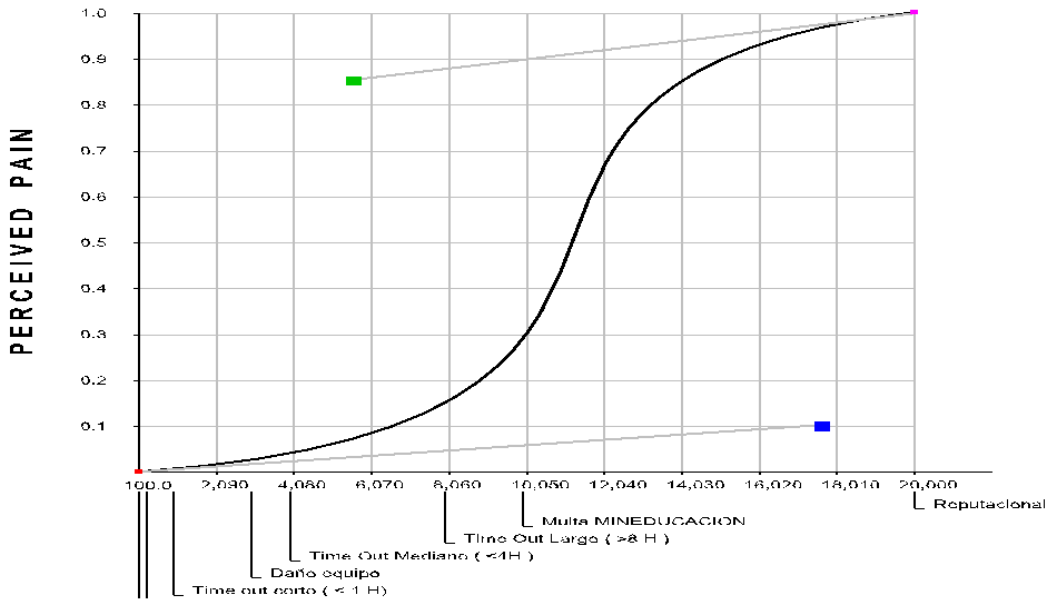



*Figura 35 Perfil de la víctima con alta tolerancia al riesgo. Elaboración propia. @SecurITree V 5.2*

Ahora es importante tener en cuenta que para priorizar las inversiones en ciberseguridad ante un ataque se propone tener en cuenta el siguiente proceso de análisis:

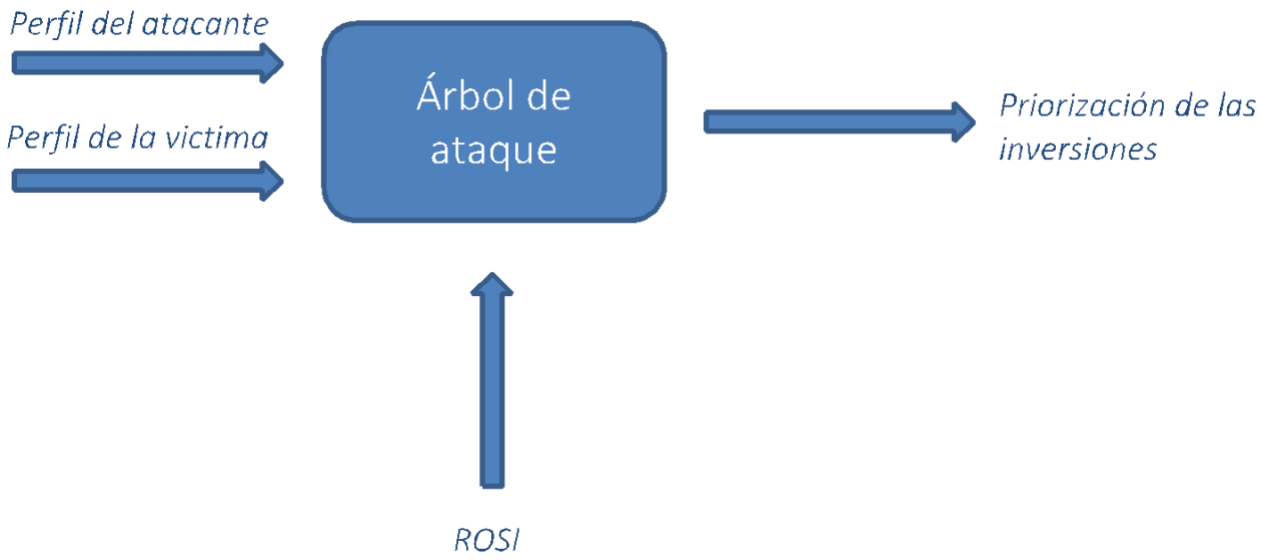



*Figura 36 Proceso para definir la priorización de inversiones. Elaboración propia del autor.*

Como variables de entrada tenemos:

- Perfil del atacante: Curvas de normalización, donde se captura la predisposición del atacante ante los costos que debe incurrir y al beneficio que recibirá. Para construir estas curvas se hace con base en la información de un panel de expertos
- Perfil de la víctima: Curvas de normalización, donde se captura el perfil de riesgo de la víctima, es decir se captura el dolor percibido ante la materialización de un ataque. Es más que la estimación de un valor absoluto del impacto. El valor absoluto del impacto de un ataque DoDS puede ser igual para las dos víctimas, pero la percepción de dolor es diferente para cada uno.
- El método para calcular el costo/beneficio de las diferentes contramedidas es el ROSI (Rentabilidad de inversiones en seguridad).

  ROSI = ((ALE *Rm)- CSI) /CSI (en términos porcentuales)

  ALE = Valor absoluto del Impacto * SRO

  SRO = Número de ataques históricos * Probabilidad de un ataque.

Rm = Riesgo residual que queda latente después de implementar la ciberseguridad.

Teniendo en cuenta que este ejercicio académico, no tenemos valores absolutos de contramedidas, lo que se hace es buscar la cantidad máximo de dinero que hay disponible para implementar la contramedida, dicho valor equivale al valor del ALE residual (ALE *Rm) que produce un ROSI = 0. Por encima de ese valor la contramedida generaría un ROSI negativo, es decir no es viable realizar dicha inversión en esa contramedida.

Para calcular el riesgo residual de las diferentes alternativas de un ataque de DoDS debemos utilizar la metodología de árboles de ataque, cumpliendo los siguientes pasos:

Primero debemos construir el árbol básico que describe las diferentes alternativas que tiene el atacante para poder realizar una denegación de servicios. Segundo, se calcula los riesgos para cada escenario del caso base, se organizan los diferentes escenarios de mayor a menor riesgo y se agrupan por las diferentes alternativas de ataque. Tercero se introduce en el árbol de ataque cada una de las diferentes contramedidas, se vuelve y se calcula el riesgo residual que queda después de introducir la contramedida, con base en estos resultados se calcula el ROSI para los escenarios de mayor altor riesgo.

Siguiendo con el proceso descrito en la Figura 18., se procede a construir el árbol de ataque, utilizando para ello la herramienta SecurItree @ Amenaza, conforme a la información recopilada en los capítulos previos y utilizando la metodología de los árboles de ataque descrito en el capítulo 3, comenzamos a construir el árbol iniciando de arriba hacia abajo. El Nodo más alto del árbol es la raíz del árbol y representa la misión del atacante, en este caso es causar la indisponibilidad de un servicio, a continuación, se presentan las diferentes alternativas para poder realizar ese ataque. Según se puede observar en la Figura 37, se realizó un diagrama que describe las alternativas como se podría llevar un ataque de DDoS, las cuales se pueden agrupar así:

- Ataque a la infraestructura de Servidores
- Ataque a la red de comunicaciones
- Ataque a la Aplicación.

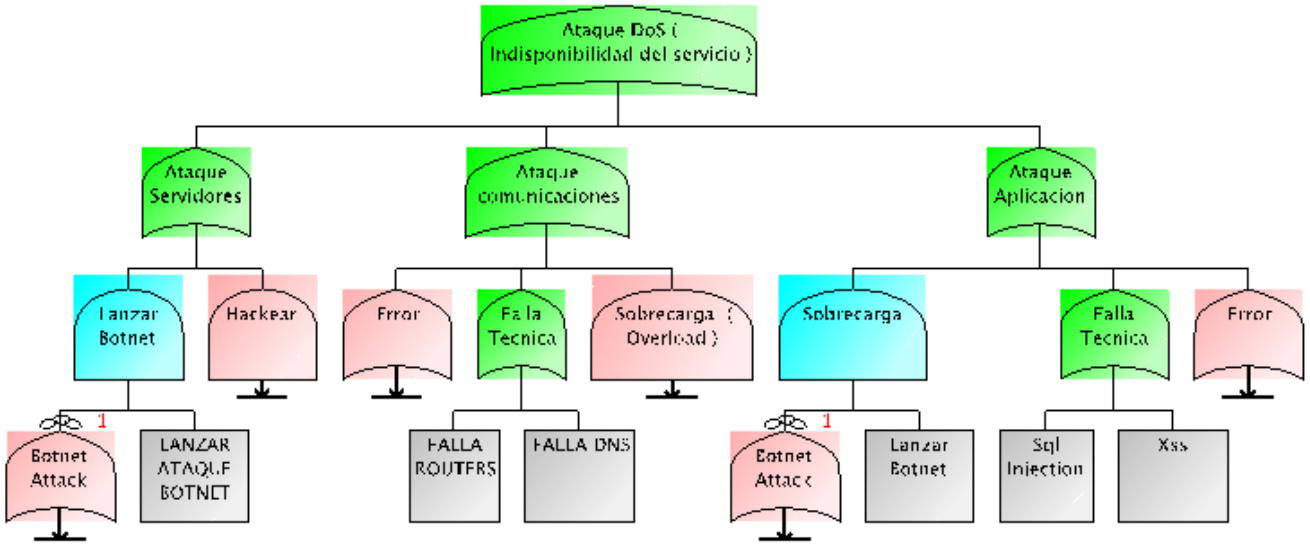



*Figura 37 (árbol de ataque DoDS). Elaboración propia. @SecurITree V 5.2.*

Después cada alternativa se desarrolla en forma más específica y detallada como el analista considere necesario para el objetivo que busca con el árbol de ataque. Entre más detalle más profundo sea el árbol, mayor será las cantidades de rutas que el atacante puede llevar a cabo, cada ruta es un escenario de ataque. Tal como se pueden observar en la Figura 38. (Descripción de un ataque de Botnet), un ataque al Sistema de comunicaciones Ver Figura 39, o un ataque al sistema a la Aplicación ver Figura 40. El ataque de BOTNET se puede describir como se observa en la Ver Figura 38

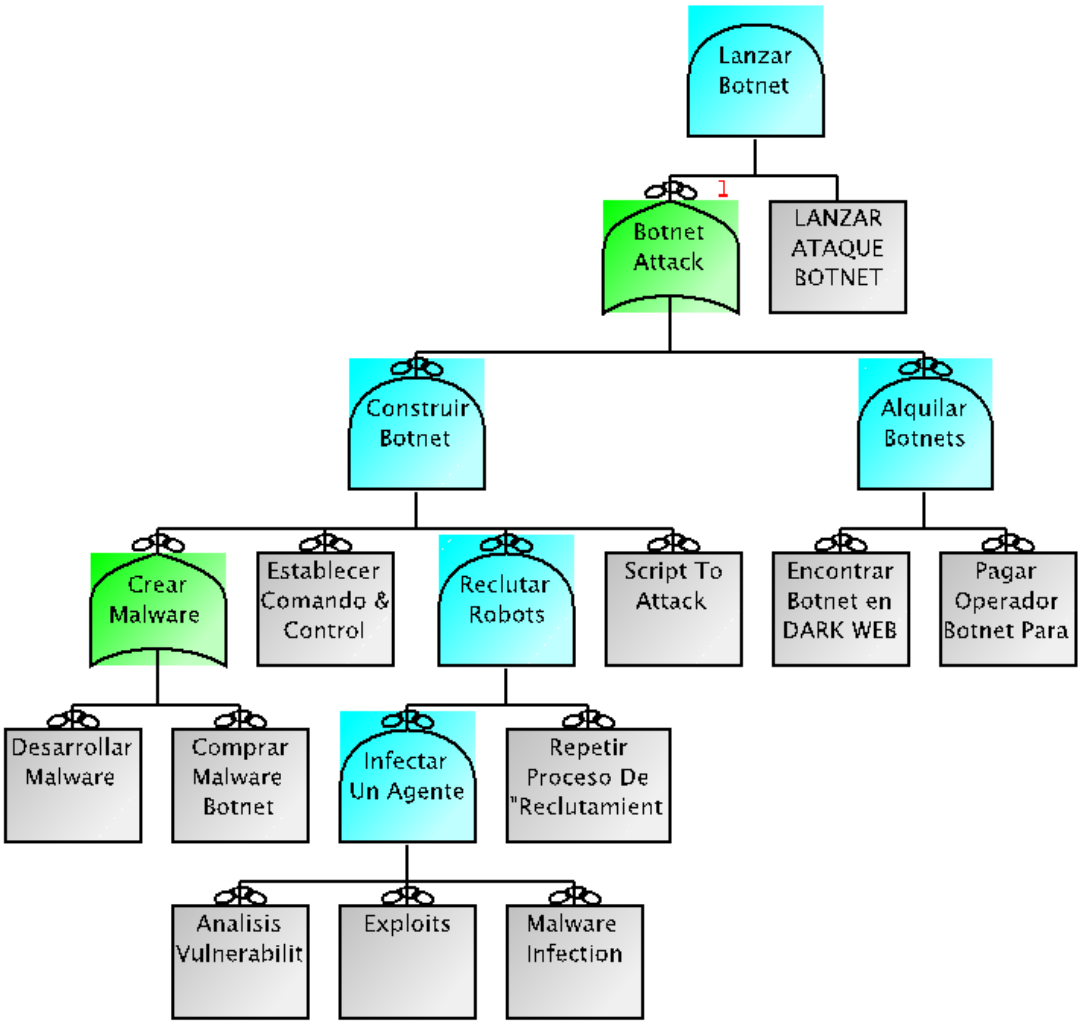



*Figura 38 Descripción de un ataque de BOTNET (Robots). Elaboración propia. @SecurITree V 5.2*

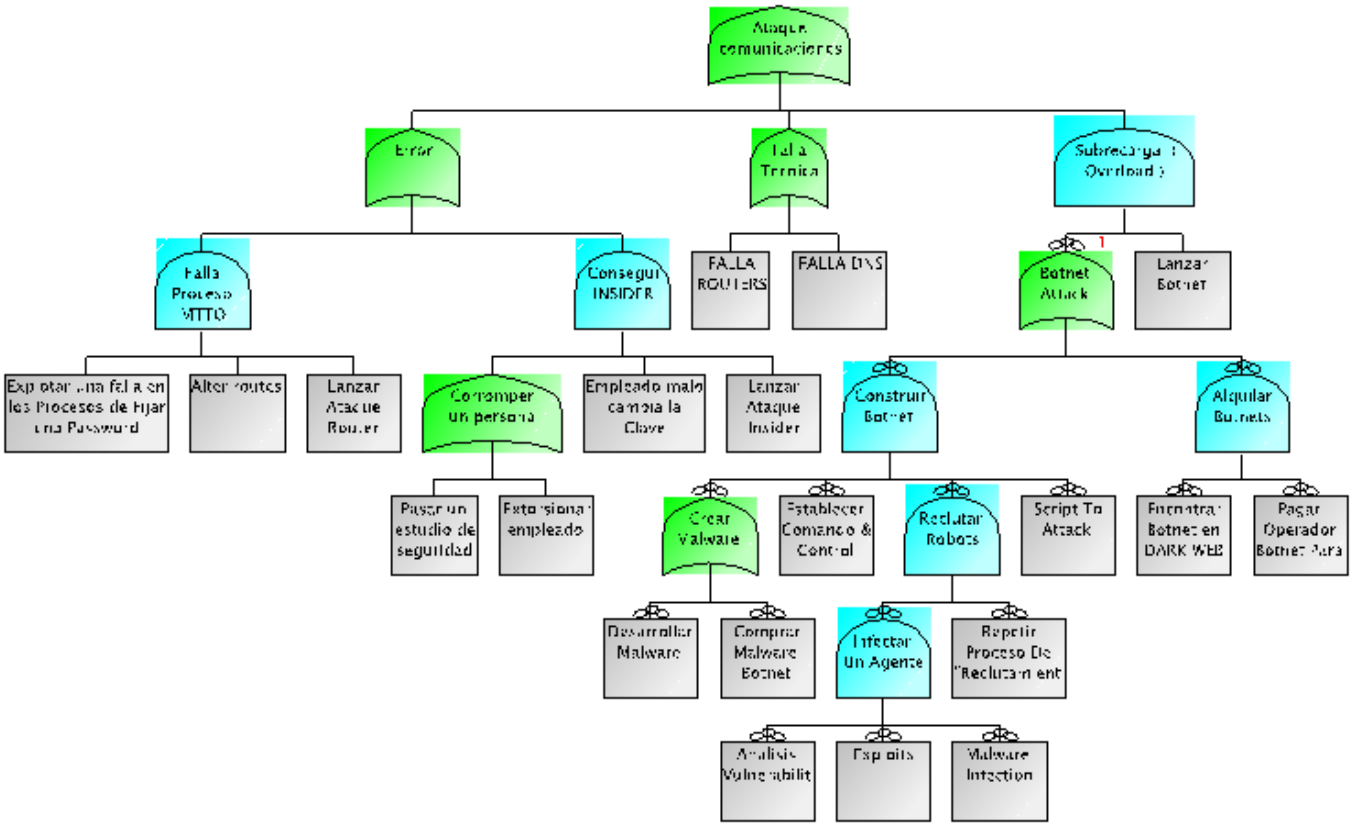



*Figura 39 Descripción de un ataque DDoS por el Sistema de comunicaciones. Elaboración propia.*

*@SecurITree V 5.2*

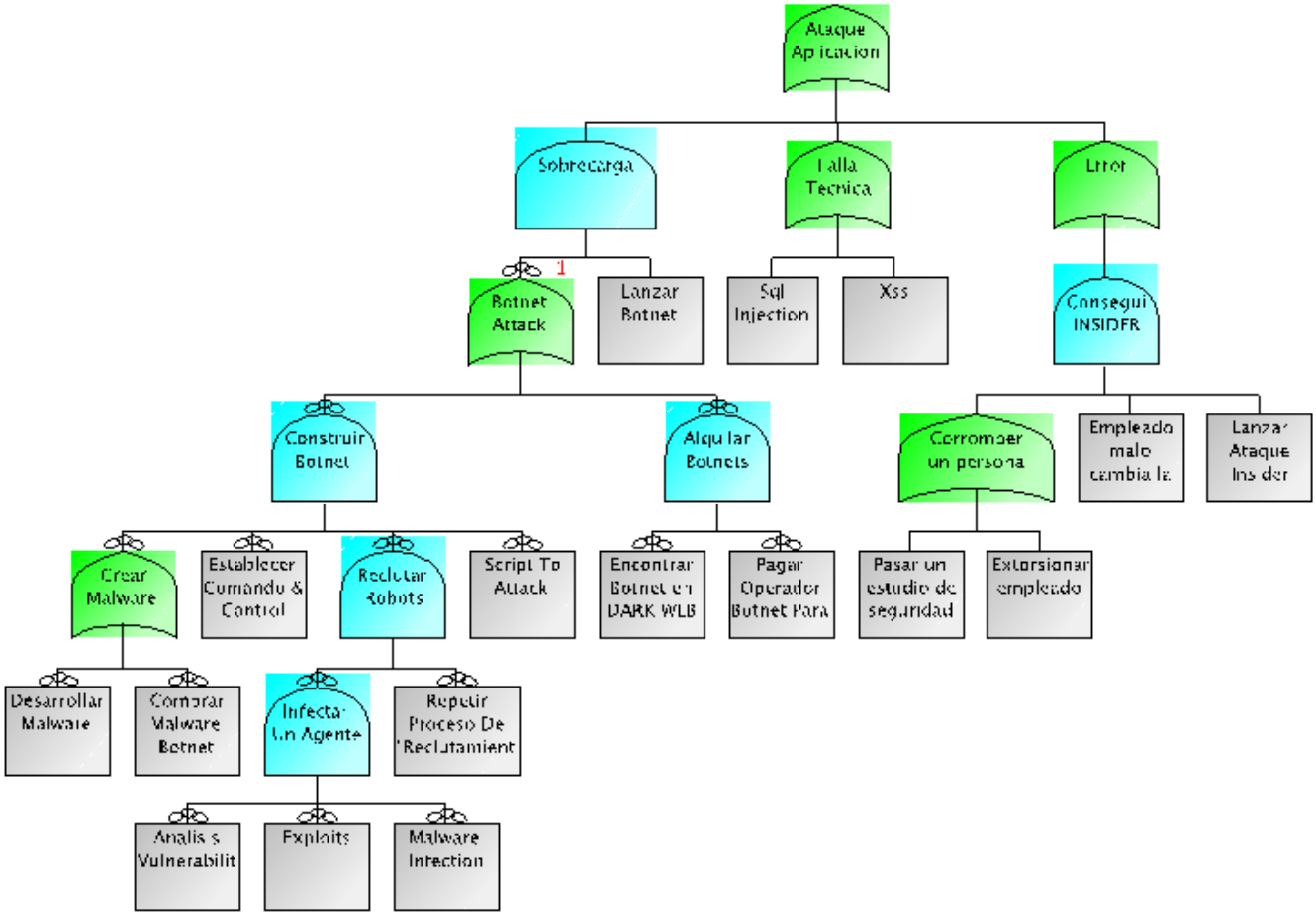



*Figura 40 Descripción de un ataque DDoS a través de la Aplicación. Elaboración propia. @SecurITree V 5.2*

Cada camino desde la base del árbol (Hojas) hasta la cúspide corresponde a un escenario posible de ataque, para cada escenario se hacen los cálculos de cúspide Probabilidad de ataque, riesgo, ALE.

En total en este Árbol resultaron 22 escenarios posibles de ataque, dichos escenarios se agruparon en 4 grupos a saber:

- Escenarios asociados a BOTNET

- Escenarios asociados a una falla del HW
- Escenarios asociados a falla Aplicación
- Escenarios asociados a un INSIDER.

Una vez se calcula el riesgo de los diferentes escenarios del árbol Base, se introducen las diferentes contramedidas. Una para cada uno de las alternativas de ataque, así:

Escenarios asociados a BOTNET – Contramedida: SIEM

Escenarios asociados a una falla del HW – Contramedida: Seguridad Perimetral

Escenarios asociados a falla Aplicación – Contramedida: WAF

Escenarios asociados a un INSIDER – Contramedida: Implementación ISO 27001.

Se introduce en el árbol de ataque dicha contramedida y se vuelve a calcular el riesgo de cada escenario. Dicho análisis se hace tanto para cada tipo de víctima y se tabulan los resultados.

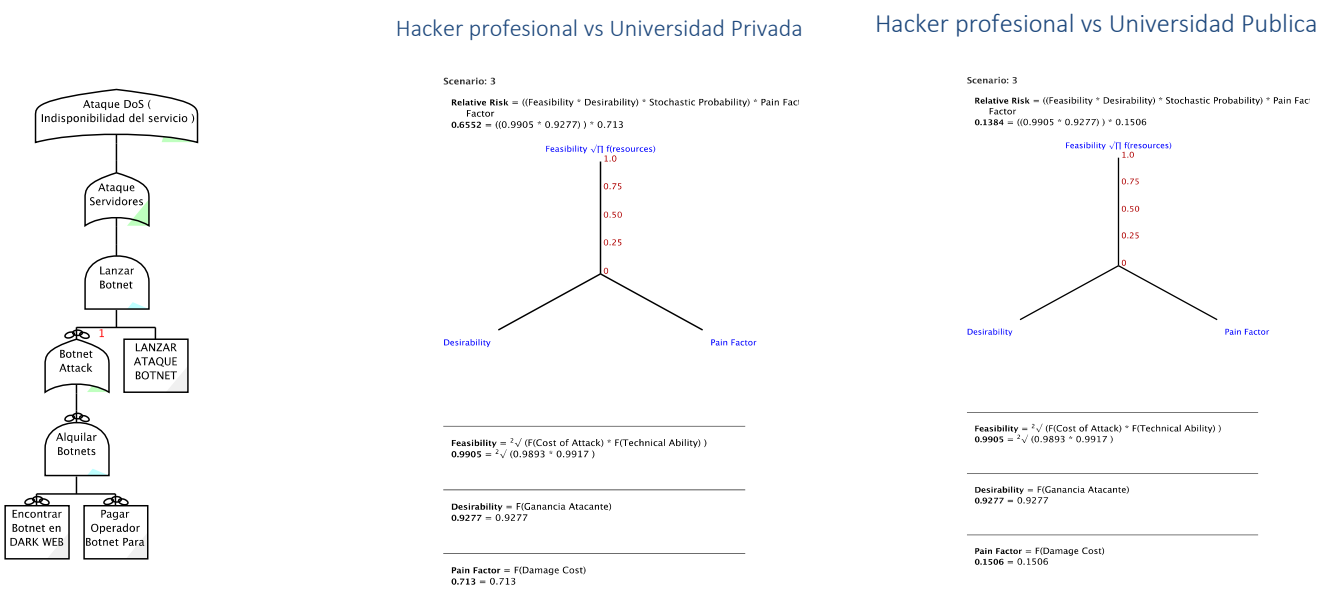



*Figura 41 Escenario de Alquilar un Botnet. Elaboración propia. @SecurITree V 5.2*

El escenario 3 es el escenario de ataque donde el atacante escoge la alternativa de alquilar un BOTNET. Se puede observar el riesgo percibido por la Universidad privada es mayor que la universidad pública. Debido principalmente a la percepción del dolor de la víctima, que ante un mismo ataque de denegación de servicio que deja la universidad 8 horas, cada uno percibe un dolor diferente. La Universidad Privada tiene una tolerancia al riesgo más baja que la universidad Pública.

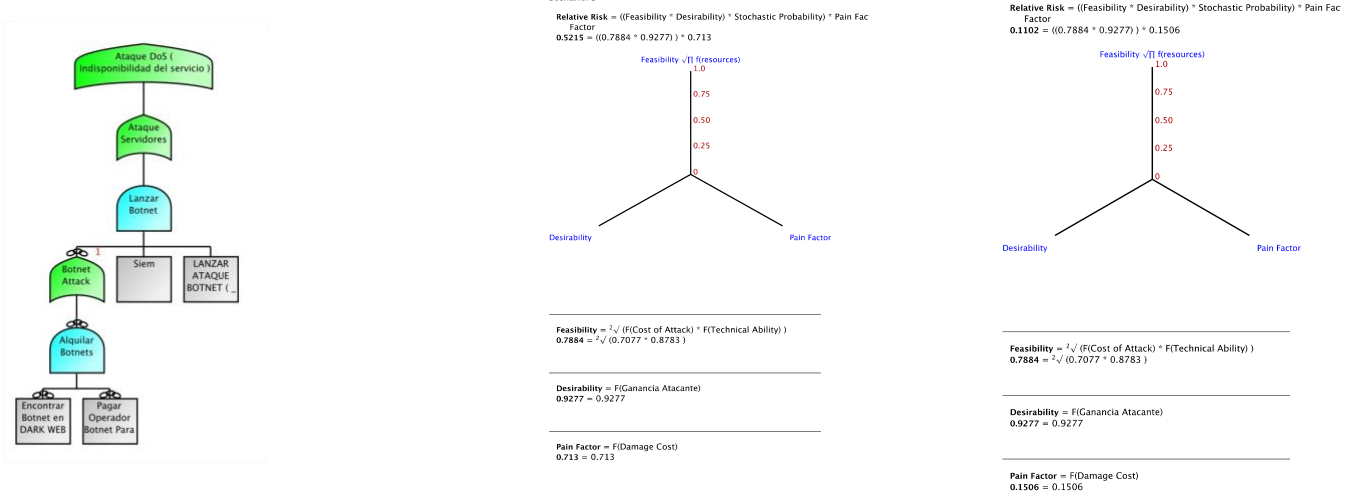



*Figura 42 Escenario Botnet – Contramedida 1 SIEM. Elaboración propia. @SecurITree V 5.2*

Para contrarrestar un ataque de BOTNET, se implementa una contramedida de un sistema correlacionado de eventos (SIEM), que permita en forma temprana permite detectar incremento inusual de tráfico y reducir el riesgo de un ataque BOTNET. Se calcula nuevamente el riesgo, tanto para cada uno de los perfiles de víctima. La diferencia de los riesgos del caso base con la contramedida es el de valor que debe alimentar el cálculo del ROSI, ver Figura 42.

HACKER PROFESIONAL vs PRIVADA
Contramedida 1 : SIEM

| ESCENARIO ATAQUE : BOTNET | | | | |
|---|---|---|---|---|
| | BASE | CONTRA 1 | Residual | % CAMBIO |
| ALE | $30,209 | $24,046 | $6,163 | 20.4% |
| RISK | 0.655 | 0.521 | 0.134 | 20.5% |
| PROB ATAQ | 0.918 | 0.731 | 0.187 | 20.4% |

ROSI =0

| | |
|---|---|
| ALE BASE | $30,209 |
| Rm | 0.134 |
| DINERO DISPONIBLE C1 | $4,048.006 |
| % ALE | 13.4% |

HACKER PROFESIONAL vs PUBLICA
Contramedida 1 : SIEM

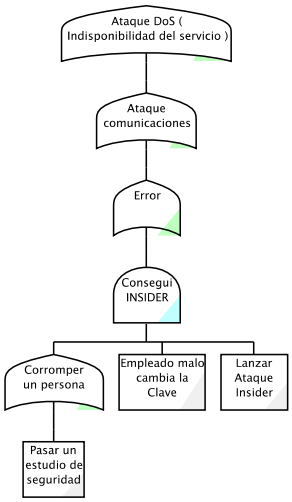
| ESCENARIO ATAQUE : BOTNET | | | | |
|---|---|---|---|---|
| | BASE | CONTRA 1 | Residual | % CAMBIO |
| ALE | $30,209 | $24,046 | $6,163 | 20.4% |
| RISK | 0.1384 | 0.1102 | 0.028 | 20.4% |
| PROB ATAQ | 0.918 | 0.731 | 0.187 | 20.4% |

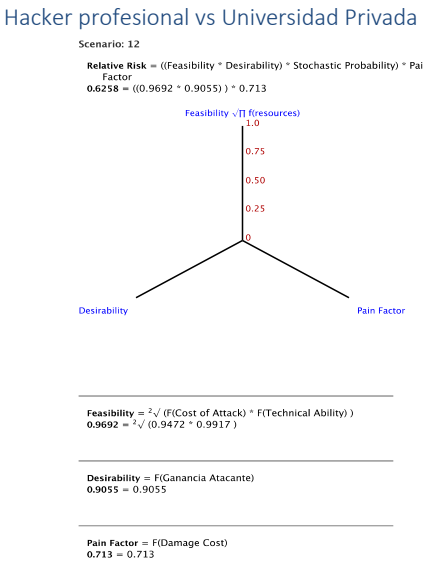
ROSI =0

| | |
|---|---|
| ALE BASE | $30,209 |
| Rm | 0.028 |
| DINERO DISPONIBLE C1 | $851.9 |
| % ALE | 2.8% |

*Figura 43 Resultados del cálculo de dinero máximo disponible para implementar SIEM. Elaboración propia.*

A continuación, revisemos los resultados de la segunda contramedida, para el escenario de un ataque donde se logra las claves de acceso debido a un infiltrado (INSIDER)



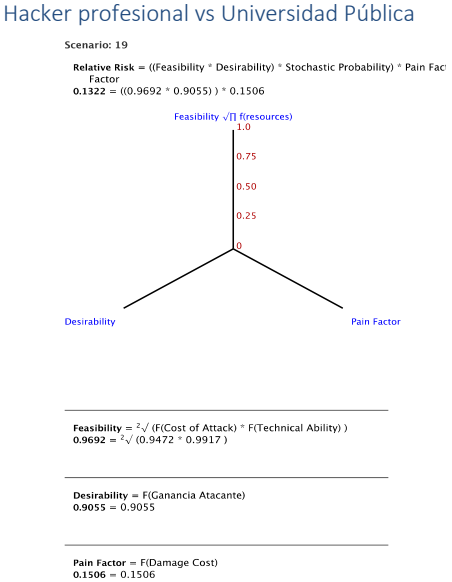




*Figura 44 Escenario de conseguir INSIDER – Elaboración propia. @SecurITree V 5.2*

Hay muchos casos donde se puede conseguir un ataque de denegación de servicios, infiltrando un delincuente dentro de la institución, es decir consiguiendo un INSIDER. Dicho INSIDER obtiene acceso a recursos privilegiados y permite que el atacante bloquee el servicio por un periodo de tiempo determinado. Tal como en el caso anterior se observa en la Figura 44 que el riesgo base es diferente para cada tipo de víctima, ya que la percepción del dolor es diferente. El riesgo es mayor para la víctima con una tolerancia al riesgo baja (Universidad Privada).

A continuación, procedemos a incluir dentro del árbol de ataque una contramedida que le dificulte al atacante introducir un INSIDER dentro de la organización. Dicha contramedida propuesta consiste en la implementación de un Sistema de gestión de ciberseguridad, tal como la ISO 27001. Dicha norma introduce controles a todos los niveles, y en este caso ayudaría a aumentar el grado de dificultad del atacante para sobrepasar dichos controles y por lo tanto disminuiría la probabilidad de un ataque por un INSIDER. Ver Figura 45.

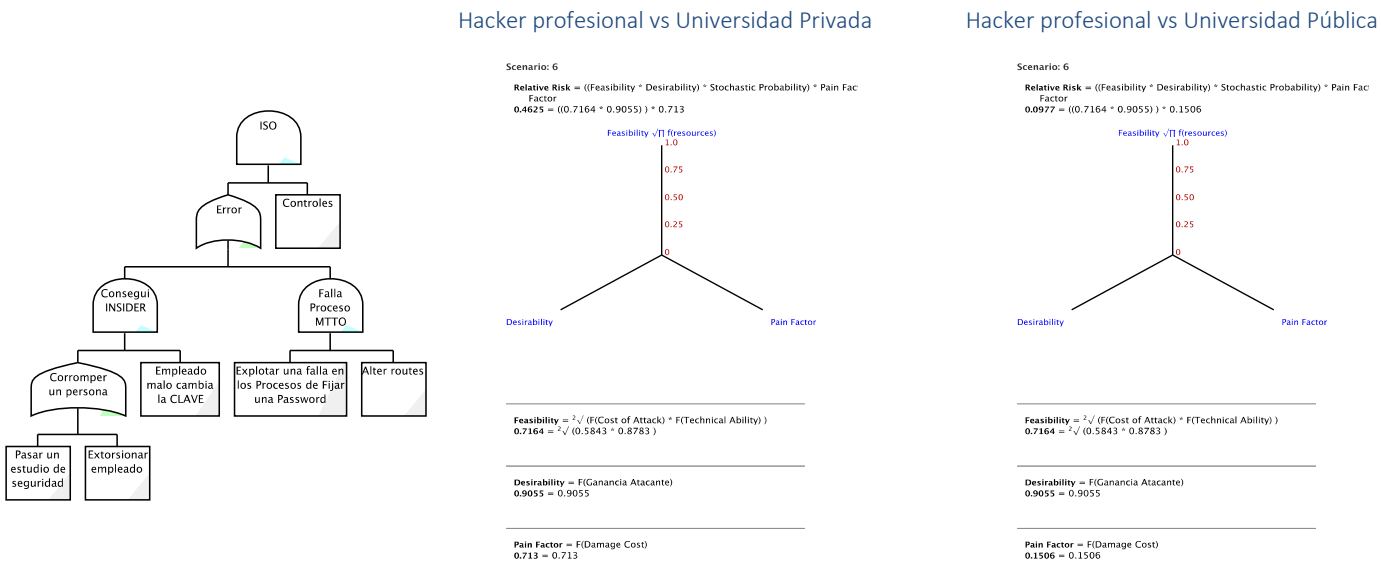



*Figura 45 Escenario INSIDER _ Contramedida ISO – Elaboración propia. @SecurITree V 5.2*

La implementación de un sistema de gestión de seguridad de la información ISO 27001, disminuye el riesgo con respecto al caso base donde no hay ninguna contramedida. Al igual que en los casos anteriores, el riesgo percibido ante un ataque de un INSIDER es menor para una víctima con una Tolerancia al riesgo más alta. (ver Figura 46). La implementación de esta contramedida genera una mayor disminución absoluta del riesgo que la contramedida de SIEM.

Hacker profesional vs. Victima Privada
Escenario INSIDER

| ESCENARIO ATAQUE : INSIDER | | | | |
|---|---|---|---|---|
| | BASE | CONTRA 4 | Residual | % CAMBIO |
| ALE | $28,854 | $21,327 | $7,527 | 26.1% |
| RISK | 0.6258 | 0.4625 | 0.163 | 26.1% |
| PROB ATAQ | 0.8776 | 0.6487 | 0.229 | 26.1% |

ROSI =0

| | |
|---|---|
| ALE BASE | $28,854 |
| Rm | 0.163 |
| DINERO DISPONIBLE C1 | $4,711.858 |
| % ALE | 16.3% |

Hacker profesional vs. Victima Publica
Escenario INSIDER

| ESCENARIO ATAQUE : INSIDER | | | | |
|---|---|---|---|---|
| | BASE | CONTRA 4 | Residual | % CAMBIO |
| ALE | $28,854 | $21,327 | $7,527 | 26.1% |
| RISK | 0.1322 | 0.0977 | 0.035 | 26.1% |
| PROB ATAQ | 0.8776 | 0.6487 | 0.229 | 26.1% |

ROSI =0

| | |
|---|---|
| ALE BASE | $28,854 |
| Rm | 0.035 |
| DINERO DISPONIBLE C1 | $995.463 |
| % ALE | 3.5% |

*Figura 46 Resultados del ALE Residual, Escenario INSIDER – Contramedida ISO. Elaboración propia.*

Ahora vamos a analizar el escenario de una falla de Servidor de DNS, el cual puede producir un error en el direccionamiento de las direcciones IP, lo que puede generar una indisponibilidad del servicio. Ver Figura 47.

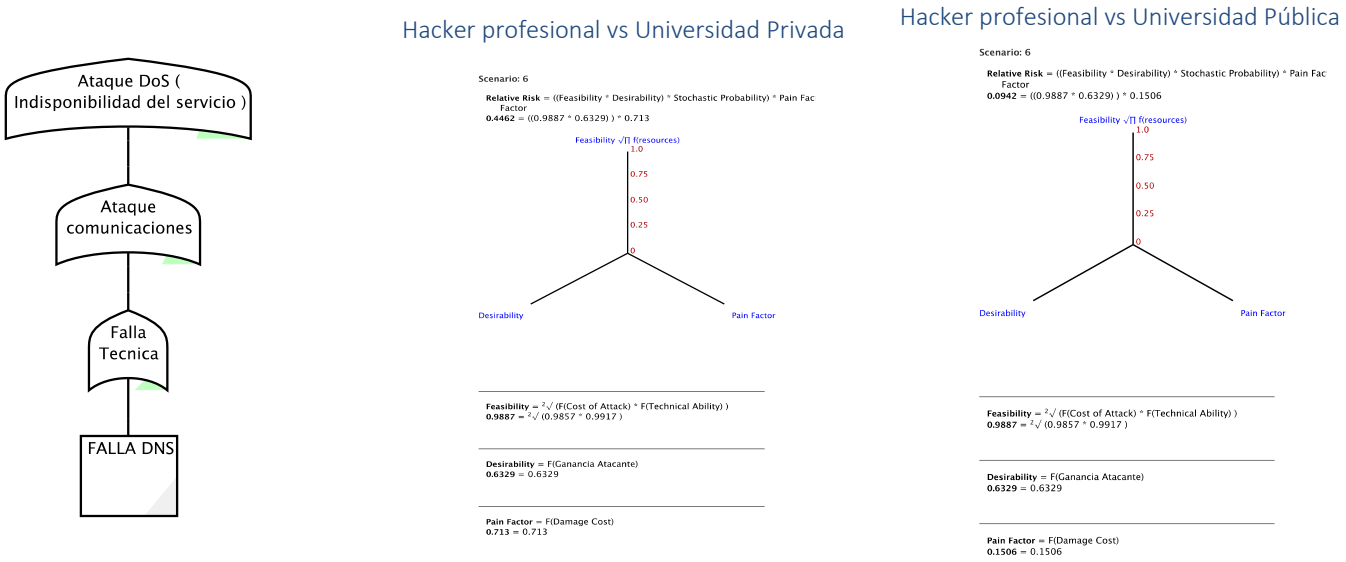
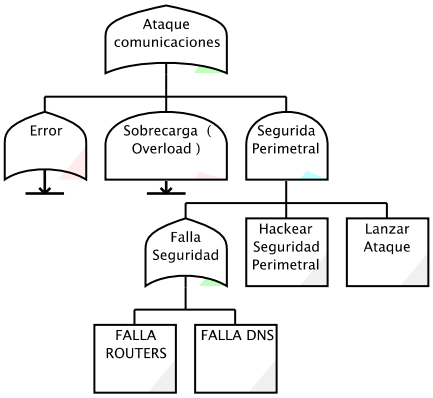
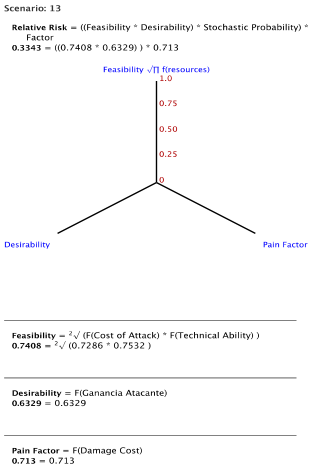



*Figura 47 Escenario de una Vulnerabilidad del Servidor DNS – Elaboración propia del autor. @SecurITree V.5.2*

Aunque el riesgo de que se presente este escenario es menor que los dos escenarios anteriores siguen siendo un escenario posible sobre todo para la víctima con una tolerancia baja al riesgo. Nuevamente es evidente, que la percepción de riesgo cambia dependiendo del perfil de la víctima. Una vez calculado el riesgo de este escenario en el caso base (sin contramedidas), se procede a calcular el riesgo introduciendo en el árbol de ataque una contramedida. Ver Figura 48.



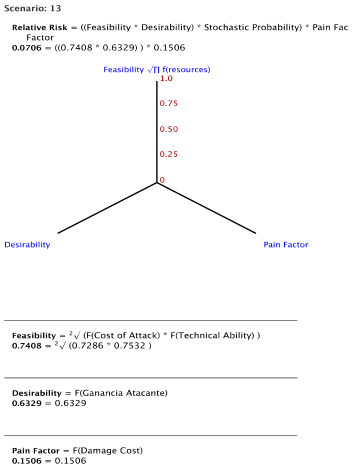




*Figura 48 Escenario falla DNS – Contramedida: Seguridad Perimetral. Elaboración propia. @SecurITree V 5.2*

En este caso se introduce una contramedida que consiste en el fortalecimiento de un sistema de seguridad perimetral con IDS / IPS, que dificultarán el trabajo de atacante para acceder al servidor del DNS, es decir eleva los costos del ataque, así como las habilidades técnicas necesarias para sobrepasar todo el sistema de seguridad perimetral. En consecuencia, la implementación de esta contramedida disminuye la probabilidad de un ataque. El riesgo residual resultante de la implementación de esta contramedida es utilizado para calcular el ALE residual que hace viable financieramente la contramedida (Ver Figura 49).

Hacker profesional vs. Victima Publica
Escenario Falla HW

| ESCENARIO ATAQUE : FALLA HW ( DNS/ ROUTER ) | | | | |
|---|---|---|---|---|
| | BASE | CONTRA 2 | Residual | % CAMBIO |
| ALE | $20,573 | $15,415 | $5,158 | 25.1% |
| RISK | 0.0942 | 0.0706 | 0.024 | 25.1% |
| PROB ATAQ | 0.6258 | 0.4689 | 0.157 | 25.1% |

ROSI =0

| | |
|---|---|
| ALE BASE | $20,573 |
| Rm | 0.024 |
| DINERO DISPONIBLE C1 | $485.523 |
| % ALE | 2.4% |

Hacker profesional vs. Victima Privada
Escenario Falla HW

| ESCENARIO ATAQUE : FALLA HW ( DNS/ ROUTER ) | | | | |
|---|---|---|---|---|
| | BASE | CONTRA 2 | Residual | % CAMBIO |
| ALE | $20,573 | $15,415 | $5,158 | 25.1% |
| RISK | 0.4462 | 0.334 | 0.112 | 25.1% |
| PROB ATAQ | 0.6258 | 0.4689 | 0.157 | 25.1% |

ROSI =0

| | |
|---|---|
| ALE BASE | $20,573 |
| Rm | 0.112 |
| DINERO DISPONIBLE C1 | $2,308.291 |
| % ALE | 11.2% |

*Figura 49 Análisis del ALE Residual – Contramedida Seguridad Perimetral. Elaboración propia.*

Como se puede observar en la Figura 49, el riesgo residual disminuye comparado con el caso base, encontrándose menos dinero disponible (ALE Residual) para implementar la contramedida del fortalecimiento de seguridad perimetral que en las dos contramedidas anteriores. Nuevamente se observa que existe menos predisposición para invertir en la victima con Tolerancia al riesgo alto. Para ese mismo ataque la Universidad Pública tiene 4,75 veces menos dinero disponible para invertir en la contramedida.

A continuación, analizamos el escenario de ataque a la aplicación, que lo hemos simplificado como un ataque vía SQL. Ver Figura 50.

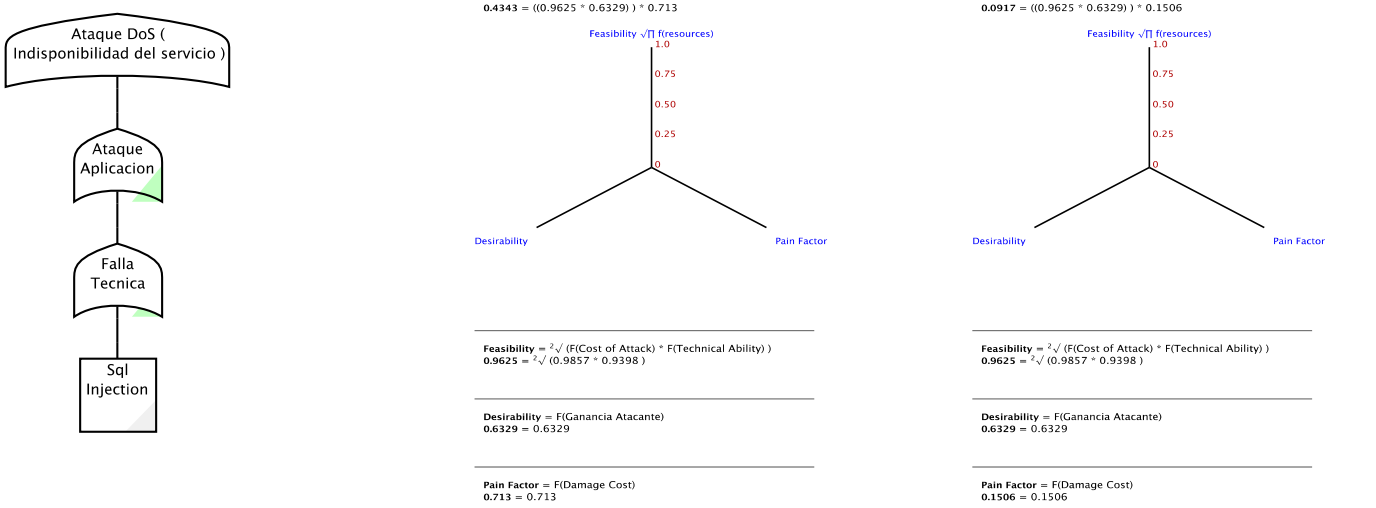



*Figura 50 Escenario de una falla en aplicación vía SQL – Elaboración propia del autor. @SecurITree V 5.2*

Tienen como objetivo una aplicación dada del nodo de la víctima, por tanto, inutilizando el uso de los clientes legítimos de esa aplicación y posiblemente saturando los recursos de la máquina. Si los recursos compartidos del nodo no son completamente consumidos, otras aplicaciones y servicios deberían ser todavía accesibles por los usuarios, por lo tanto, son difíciles de detectar. Para efectores prácticos hemos simplificado un tipo de ataque vía SQL, donde el atacante pretende tener acceso a las claves de los usuarios legítimos y desde allí perpetrar el ataque. Otro tipo de ataque a la capa 7 (Aplicación) es vía un ataque al protocolo HTTP, donde se inunda con mensajes HTTP GET, HTTP POST, etc. Este escenario arroja un nivel de riesgo similar al de un ataque al servidor de DNS. Tal como se observa en la Figura 51, el riesgo de la víctima con mayor tolerancia al riesgo (U Pública) percibe un riesgo menor que la víctima con menor tolerancia al Riesgo.

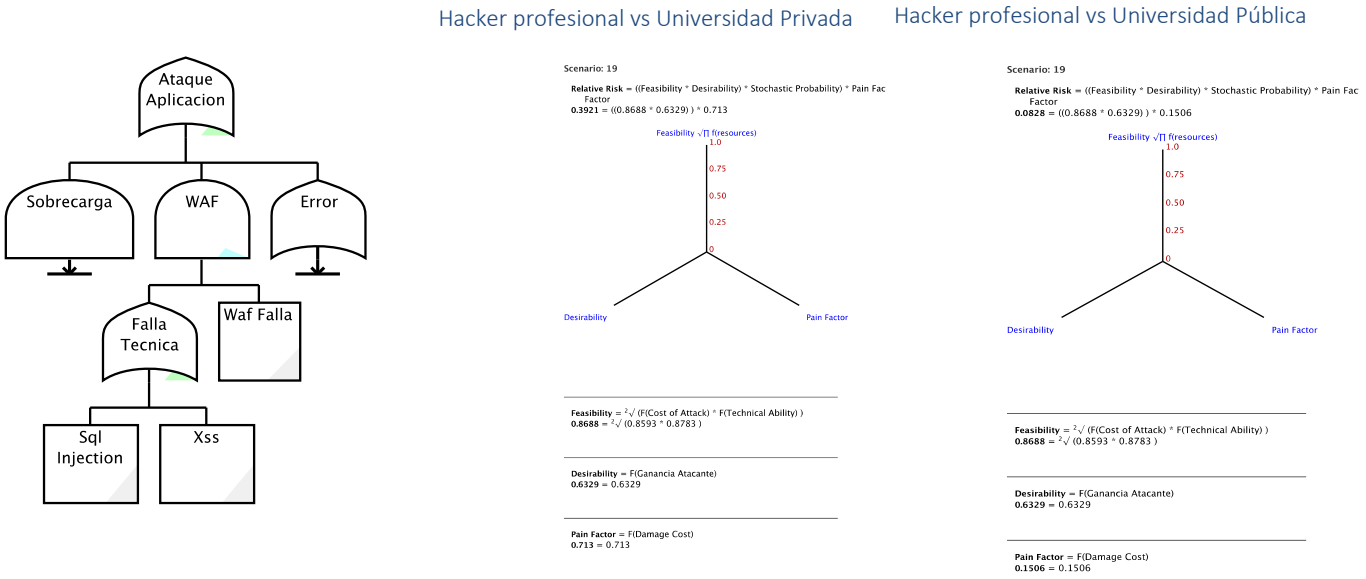



*Figura 51 Escenario Falla aplicación-SQL – Contramedida WAF @SecurItree V5.2*

Para este tipo de ataques a la aplicación al servidor web, se recomienda la implementación de una contramedida para proteger la aplicación mediante la instalación de un WAF (por sus siglas en ingles “Web Aplicación Firewall “) que tiene como objetivo proteger contra múltiples ataques al servidor Web. La función del WAF es garantizar la seguridad del servidor web mediante el análisis de paquetes HTTP/ HTTPS y modelos de tráfico. Como se puede observar dicha contramedida reduce el riesgo en una porción menor que los casos anteriores, pero muy similar al caso del escenario del ataque al servidor DNS. Debido a que la diferencia porcentual del cambio de la probabilidad de un ataque a la aplicación es menor que para el caso del DNS.

Hacker profesional vs. Victima Privada
Escenario Falla APLICACION

| ESCENARIO ATAQUE : FALLA APLICACIÓN ( SQL ) | | | | |
|---|---|---|---|---|
| | BASE | CONTRA 3 | Residual | % CAMBIO |
| ALE | $20.027 | $15.035 | $4.992 | 24,9% |
| RISK | 0,4343 | 0,3261 | 0,108 | 24,9% |
| PROB ATAQ | 0,6092 | 0,4573 | 0,152 | 24,9% |
| | | | | |
| ROSI =0 | | | | |
| | ALE BASE | | $20.027 | |
| | Rm | | 0,108 | |
| | DINERO DISPONIBLE C1 | | $2.166,9 | |
| | % ALE | | 10,8% | |

Hacker profesional vs. Victima Publica
Escenario Falla APLICACION

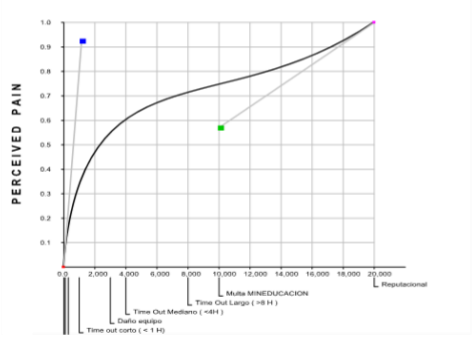
| ESCENARIO ATAQUE : FALLA APLICACIÓN ( SQL ) | | | | |
|---|---|---|---|---|
| | BASE | CONTRA 3 | Residual | % CAMBIO |
| ALE | $20.027 | $15.035 | $4.992 | 24,9% |
| RISK | 0,0917 | 0,0689 | 0,023 | 24,9% |
| PROB ATAQ | 0,6092 | 0,4573 | 0,152 | 24,9% |
| | | | | |
| ROSI =0 | | | | |
| | ALE BASE | | $20.027 | |
| | Rm | | 0,023 | |
| | DINERO DISPONIBLE C1 | | $456,6 | |
| | % ALE | | 2,3% | |

*Figura 52 Análisis de ALE residual con la contramedida WAF. Elaboración propia.*

El dinero disponible para implementar esta contramedida es menor que la contra si agrupamos los resultados obtenidos para cada contramedida, podemos priorizar las inversiones como se puede observar en la Figura 53

Priorización de inversiones
Hacker profesional vs. Victima Privada

| CONTRAMEDIDAS | DINERO ( ROSI =0 ) | % ALE |
|---|---|---|
| CONTRA 4 ( ISO ) | $4,711.858 | 16.3% |
| CONTRA 1 ( SIEM ) | $4,048.006 | 13.4% |
| CONTRA 2 ( PERIMETRAL ) | $2,308.291 | 11.2% |
| CONTRA 3 ( WAF ) | $2,166.9 | 10.8% |




Priorización de inversiones
Hacker profesional vs. Victima Publica

| CONTRAMEDIDAS | DINERO ( ROSI =0 ) | % ALE |
|---|---|---|
| CONTRA 4 ( ISO ) | $995.463 | 3.5% |
| CONTRA 1 ( SIEM ) | $851.894 | 2.8% |
| CONTRA 2 ( PERIMETRAL ) | $485.523 | 2.4% |
| CONTRA 3 ( WAF ) | $456.6 | 2.3% |

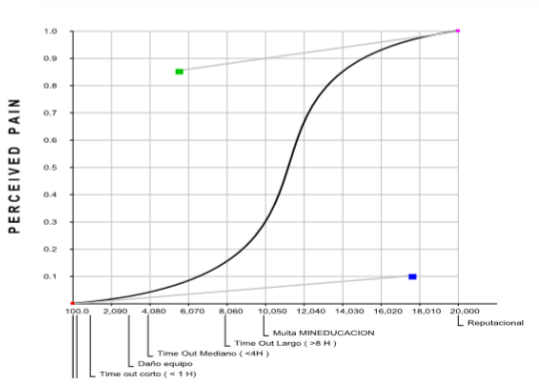



*Figura 53 Resultados Priorización de Inversiones Hackers Profesional vs Victima Privada,*

*Priorización de Inversiones Hacker Profesional vs Victima Pública. Elaboración propia. @SecurITree V 5.2*

Según este análisis, que prioriza las inversiones acorde a la cantidad de riesgo mitigado, el control (contramedida) que tiene más prioridad consiste en la implementación de un sistema de gestión de seguridad informática, ya que esto eleva los recursos que un atacante debe invertir para sobrepasar los controles impuestos para evitar la presencia de un INSISDER y disminuir los errores debidos a fallas en los procesos de mantenimiento, es decir, va disminuir la probabilidad de un error humano que es el eslabón más débil de la cadena de protecciones en cualquier sistema de ciber-seguridad. En segunda prioridad la contramedida que implementa un sistema correlacionado de eventos (SIEM) que permite detectar un incremento de tráfico ilegal en las etapas tempranas del ataque. En tercer lugar, está el fortalecimiento del sistema de seguridad perimetral con IDS / IPS. Finalmente, en el cuarto lugar de prioridad, está la inversión en una contramedida del WAF.

Es importante anotar que, debido a la tolerancia al riesgo de cada una de las víctimas, la victima que es más tolerante al riesgo, está dispuesta a invertir menos dinero en las mismas contramedidas.

# 4. CAPITULO IV

## 4.1. Conclusiones

1. Los árboles de ataque son una metodología que nos permite modelar un ataque en forma flexible ya que; permite describir el nivel detalle del ataque acorde al objetivo buscado, permite calcular el riesgo para cada escenario de ataque, es un método fácil de usar extremadamente visual, lo cual facilita la presentación en auditorios de decisión donde no se tiene un conocimiento especializado, pero aprueban un presupuesto de inversión en universidades y empresas; además es la única metodología de amenazas, que permite modelar victimas con diferentes perfiles de tolerancia al riesgo y medir su efecto en la toma de decisiones de inversiones en ciberseguridad.
2. La expectativa anual de perdida (ALE, por sus siglas en inglés) cambia conforme la probabilidad de ataque cambia, puesto que hay una correlación positiva en la expectativa de pérdida y la probabilidad de una amenaza se materialice. Es decir, el ALE disminuye con la introducción de una contramedida, ya que se disminuye la probabilidad de un ataque.
3. La probabilidad de un ataque depende de las brechas de seguridad (vulnerabilidades de la víctima) lo cual consume recursos del atacante, pero también de los beneficios percibidos por el atacante. No depende del perfil de tolerancia al riesgo de la víctima.
4. La percepción de riesgo ante un ataque cibernético una institución educativa, expuesto ante un mismo perfil de atacante, depende del perfil de riesgo de la víctima. Dos instituciones expuestas antes la amenaza de un ataque de denegación de servicios, reaccionan en forma diferente debido a su tolerancia al riesgo.
5. Víctimas con tolerancia al riesgo baja, están dispuestos a invertir más dinero en contramedidas de ciber seguridad que una institución con tolerancia al riesgo alta. Nos es lo mismo estar fuera de servicio 8 horas en una víctima privada con una baja tolerancia al riesgo que una víctima pública con una alta tolerancia al riesgo.
6. La prima de riesgo de una aseguradora sería más costosa para una víctima con alta tolerancia al riesgo ya que su disposición a invertir en contramedidas es baja.

**Recomendaciones.**

1. Se recomienda seguir explorando en el uso de la herramienta de árboles de ataque para analizar el impacto que puede tener en la disminución de los ataques la tolerancia al riesgo del atacante, lo cual puede variar de país a país, donde las los procesos penales pueden ser más expeditos y las penalidades pueden ser más fuertes, tal que disminuya su voluntad a realizar al ataque por el temor a ser capturado y procesado legalmente.
2. Explotar los beneficios de las herramientas de árboles de taque para cuantificar en forma más precisa el riesgo, usando fórmulas matemáticas y lógicas que ayudan al decisor soportar sus decisiones con base en números.
3. Incluir dentro de la materia de gestión gerencial de ciberseguridad, el estudio de los árboles de ataque para incrementar el conocimiento y descripción de un ataque de ciberseguridad. Así como en este caso se presentó un caso de uso para un ataque de DDoS, dicha herramienta permita modelar cualquier tipo de ataque, permitiéndole al estudiante profundizar sobre la forma como se puede llevar a cabo dicho ataque.
4. Estudiar la posibilidad de usar herramienta del árbol de ataque para el cálculo de la prima de riesgo que una empresa de seguros puede cobrar por una póliza de ciberseguridad.
5. Crear un grupo de investigación en optimización de inversiones en ciberseguridad, ya que la seguridad se incrementa en proporción a las inversiones, pero el gradiente de la relación costo / beneficio crece hasta determinado punto, a partir del cual ya este gradiente comienza disminuir. Incluir en este análisis de optimización el perfil de riesgo de la víctima es un reto interesante.

## 5. REFERENCIAS


1. "Las 7 fases de un ciberataque ¿Las conoces?". Colombia: Instituto Nacional de Ciberseguridad.

   http://www.belt.es/expertos/CIP_report_final_es_fnl_lores.pdfJiménez, A. (2020).
2. Albanese, D. (2012). Análisis y evaluación de riesgos: aplicación de una matriz de riesgo en el marco de un plan de prevención contra el lavado de activos.
3. Alberts C, Dorofee A, Steve J. "Introduction to OCTAVE Approach, Software Engineering Institute, Carnegie Mellon University, Pittsburg .PA-2003 "
4. Alemán Novoa, H., y Rodríguez Barrera C. (2015). "Metodologías para el análisis de riesgos en los sgsi". *Publicaciones e Investigación* 9:73.
5. Alquiler de botnets (2010). "Chinese Botnet Herders Offer 'Commercial' DDoS Services" Recuperado de: http://blog.executivebiz.com/2010/09/chinese-botnet-herders-offer-commercial-DDoS- services/
6. Alquiler de botnets (s.f). Botnet DDoS Attacks. Recuperado de: http://www.incapsula.com/DDoS/DDoS-attacks/botnet-DDoS
7. Alquiler de botnets. (2012). DDoS for hire services offering to 'take down your competitor's web sites' going mainstream. Recuperado de: http://blog.webroot.com/2012/06/06/DDoS-for-hire-services-offering-to-take-down-your- competitors-web-sites-going-mainstream/
8. Anchundia, C. (2017). Ciberseguridad en los sistemas de información de las universidades. *Revista Científica Dominio de las Ciencias*, 3(2), 200-217.

9. Angulo, C (2020) Modelo para Medir el retorno sobre la inversión en seguridad informática y de la información – ROSI. Universidad Nacional Abierta y a Distancia
10. Baker, S., Waterman, S. & Ivanov, G. (S.f). En el punto de mira las infraestructuras
11. Barba Olivares, G. (2017). "Modelado de Amenazas, una Técnica de Análisis y Gestión de Riesgo Asociado a Software y Aplicaciones". *Universidad Piloto de Colombia* 1–12.
12. Barrios, D, Del Rio, E y Esguerra Estarita, F. (2006). *Guía para implementación de seguridad en aplicaciones web y de escritorio basada en tecnologías.net*. Universidad Tecnológica de Bolívar.
13. Behara, R., Huang, C. Derrick; and Hu, Qing. (2007) "A System Dynamics Model of Information Security Investments". ECIS 2007 Proceedings. 177.
14. Bella, G. Bistarelli S. Peretti, P. et. (2007) "Augmented Risk Analysis".
15. Betancourt, R., Monroy, P. C. & Davila, J. C. (2015). *Implementación de sistemas de control de la información en el Sena regional Tolima*. Trabajo de grado. Institución Universitaria Politécnico Grancolombiano, Bogotá.
16. Bistarelli, Fioravanti & Peretti (2006) Defense trees for economic evaluation of security investments. Universit`a degli Studi "G. d'Annunzio
17. Bodeau, D, y Graubart, R. (2013). "Characterizing effects on the cyber adversary". *Mitre Technical Report Mtr130432* (November).
18. Bodeau, D., Mccollum, C. & Fox, D. (2018). Cyber Threat Modeling: Survey, Assessment, and Representative Framework.

19. Boldt, M., Carlsson, B. & Jacobsson, A. (2010). Explorando los efectos de spyware. *Revista Científica, 1*(2), 1- 9.
20. Brunner, J., Tedesco, J. C. & Aylwin, M. (2003). *Las nuevas tecnologías y el futuro de la educación*. Colombia: Grupo Editor.
21. Caballero A (2013) Information security essentials for IT managers: Protecting mission-critical systems. Managing Information Security, 2nd Edition
22. Cabeza, M. Cabrita, E. (2006). Análisis de riesgo cuantitativo de procesos: clave de la planificación estratégica.
23. Cano, J. (2016). *Fraude de informático: Viejos trucos nuevos entornos*. (1ª. ed.). Colombia: Editorial Acis.
24. Castellaro, M., Romaniz, S. & Ramos, J. C. (2013). ¿Qué hay respecto a atender a la Seguridad durante el desarrollo de sistemas de información? Revista de la Universidad Tecnológica Nacional, 2(2), 1 – 12. Recuperado de http://conaiisi.unsl.edu.ar/2013/147-486-1-DR.pdf
25. Castellaro, M., Romaniz, S. & Ramos, J. C. y Gaspoz, I. (2016). "Aplicar el Modelo de Amenazas para incluir la Seguridad en el Modelado de Sistemas". *V Congreso Iberoamericano de Seguridad Informática-CIBSI* (July):16.
26. Castro, J. Porras, L. (2020). Riesgos Residuales.
27. Cole E (2013) Advanced Persistent Threat Understanding the Danger and How to Protect Your Organization. 225 Wyman Street, Waltham, MA 02451, USA
28. Conrad, Misenar & Feldma, (2014) Eleventh hour CISSP: study guide
29. Dadkhah, M., Ciobotaru, A. M., Davarpanah, M. & Barati, E. (2014). Una introducción a los keyloggers indetectables con pruebas experimentales. *Revista*

*Internacional de Redes de Computadores y Seguridad de las Comunicaciones, 4*(3), 1- 5.

30. Donoso, Y. (2018). El reto de los cambios tecnológicos como base de las transformaciones. *Revista Forosisis de la Universidad de los Andes, 8*(2), 1- 64.
31. Dzarma, Abdulkadi & Idama, (2015) Risk Management of Some Machines in Centre for Equipment Maintenance and Industrial Training (CEMIT) in Modibbo Adama University of Technology, Yola
32. Echaiz, J. & Ardenghi, J. (2015). Detección de spoofing en paquetes IP. *Revista Científica, 2*(2), 1- 5.
33. Esplandiu, J. (2017). *Cuadernos de seguridad: Seguridad en los centros universitarios*. (1ª. ed.). Colombia: Editorial Ediciones S.A.S.
34. Estrada, C. (2017). "Modelado de un ataque con Árboles de Ataque - Sothis". Recuperado el 16 de septiembre de 2020 (https://www.sothis.tech/modelado-ataque-Árboles-ataque/).
35. González, M. (2014). *Fraudes en internet y estafa informática.* Trabajo de grado. Universidad de Oviedo. España.
36. Gregg, M. (2007) "CISA Exam Prep: Certified information systems auditor. (1ª. ed.)."
37. Gros, B. (2015). Pensar sobre la educación desde una concepción sistémico-cibernético. *Revista Teoría de la Educación, 8*(2), 81-94.
38. Guigui, R. Salas, H. (2012). El valor presente neto en riesgo - Una nueva medida fundamental para la aceptación o rechazo de proyectos de inversión.

39. Haque & Keffeler, and T. Atkison. (2017) “An Evolutionary Approach of Attack Graphs and Attack Trees: A Survey of Attack Modeling”. in The International Conference on Security and Management (SAM),
40. Hathaway M, et al (2018) Gestión del riesgo: Cibernético nacional. White paper series Edición 2
41. Hernandez, A. Cornejo, D. Callis, E. (2006). Utilización del Método de Arboles de Eventos para Evaluar la Seguridad de Instalaciones Radiactivas.
42. Herraez, F. Acuña, L. (2009). El Análisis Modal de Fallos y Efectos: una primera aproximación a su aplicación en la industria del aserrado de la madera en rollo.
43. Holtsnider & Jaffe (2012) IT Manager's Handbook: Getting your new job done. Third Edition https://aisel.aisnet.org/ecis2007/177
44. Informe MCAFEE CIBERGURRA (s.f): http://www.belt.es/expertos/CIP_report_final_es_fnl_lores.pdf
45. Kaspersky 2020: Ataques DoDS. Ataques DDoS en el primer trimestre de 2020 | Securelist
46. Kaspersky. (2016). *Boletín de seguridad de Kaspersky 2016: Historia del año: la revolución del ransomware*. USA: Infortec.
47. Kaspersky. (2018). *Boletín de seguridad Kaspersky: Kaspersky Lab predicciones sobre amenazas para el 2018*. USA: Infortec.
48. Kaspersky. (2020). Boletín de seguridad Kaspersky: Kaspersky Lab predicciones sobre amenazas para el 20. USA: Infortec.
49. Kumar, A & Fatema (2014) A Quantitative Measurement Methodology for calculating Risk related to Information Security

50. L. Martin. (2015) “Gaining the Advantage: Applying Cyber Kill Chain Methodology to Network Defense”. Lockheed Martin Corporation,
51. León, C. A. & Bonilla, M. A. (2017). *Análisis de ataques informáticos mediante honeypots para el apoyo de actividades académicas en la Universidad Distrital Francisco José de Caldas*. Proyecto de Grado para optar por el título de ingeniero en telemática. Universidad Distrital Francisco José de Caldas, Bogotá D.C.
52. Lopera, L. H. (2020). *Cibercultura crítica universitaria: el poder de transformar la sociedad informatizada Una propuesta desde el enfoque de las pedagogías decoloniales para orientar la formación crítica universitaria en la era digital.* Trabajo de grado para optar al título de magister en educación. Universidad de Antioquia, Bogotá D.C.
53. Magar, A. (2016). “State-of-the-Art in Cyber Threat Models and Methodologies”. *Sphyma Security* (March).
54. Mirkovic Jelena, Reiher Peter, (2004). A taxonomy of DDoS attack and DDoS Defense mechanisms
55. Moncayo, D. (2014) Modelo de evaluación de riesgos en activos de tic’s para pequeñas y medianas empresas del sector automotriz
56. Montealegre, S. (2018). “Análisis relación costo/beneficio de la implementación del proyecto de renovación tecnológica (pri ii) en el grupo empresarial coomeva usando el modelo total cost of ownership (tco)”.
57. Muñoz, M., Salazar, S. & Yang, P. (2016). *Seguridad de la información: ARP Spoofing*. Trabajo de grado. Universidad Técnica Federico Santa María. Chile.

58. Niño, Y. (2015) Importancia de la implementación del concepto de ciberseguridad organizacional en las organizaciones tipo PYMES
59. Ochoa, M. (2019). Análisis cualitativo y cuantitativo de los riesgos que influyen en el cronograma y el presupuesto.
60. Oosthuizen, R., Pretorius, L., Mouton, F., Molekoa, M. (2019) Cyber security investment cost-benefit investigation using system dynamics modelling
61. Osborne M (2006) How to cheat at managing information security: Jargon, principles, and concepts
62. Plaza, J. A. (2019). "¿Rompiendo la Cadena del Cyber Kill Chain?" *Articulo para materia Sistemas Cibernéticos.* Escuela Superior de Guerra. Bogotá, Colombia.
63. Pols, Paul. 2017. *The Unified Kill Chain Designing a Unified Kill Chain for analyzing, comparing and defending against cyber-attacks*.
64. Porras, H. (2018). Supercomputación, el camino hacia la independencia tecnológica. Revista Forosisis de la Universidad de los Andes, 8(2), 1- 64.
65. Puga, M (2019) VAN y TIR. Universidad Arturo Prat del Estado de Chile. Chile
66. Quiroga, M. (2018). 2Seguridad (Resiliencia) en el ciclo de vida del software. (1ª. ed.)." Colombia: Ediciones SAS.
67. Ramírez, R. (2017). *Entendiendo los Ciber-Ataques - Parte I. The Cyber-Kill Chain*.
68. Ramón, J. (2016). Nuevo espacio de educación superior en ciberdefensa en el ámbito internacional. *Revista Formación, 2*(120), 116- 118.
69. Reguant, M. Torrado M. (2016). El método Delphi.
70. Reza Esmaeili, S., & Soltani Esterabadi, A. (2019). Attack Analysis Methodologies Attack Analysis Methodologies in the Automotive Industry., Master's Thesis,

Chalbers University – Sweden: Attack Analysis Methodologies in the Automotive Industries.

71. Rosenquist M (2008) Defense in Depth Strategy Optimizes Security
72. Roumani M, et al (2015) Value Analysis of Cyber Security Based on Attack Types.
73. Saitta, Paul, Brenda Larcom, y Michael Eddington. 2005. *Trike v.1 Methodology Document [Draft]*.
74. Sánchez, G. (2011). *Delitos en internet: clases de fraudes y estafas y las medidas para prevenirlos*. España: Editorial Universidad Complutense de Madrid.
75. Sastoque, D. & Botero, R. (2015). Técnicas de detección y control de phishing. *Revista Cuaderno Activa, 7*(2), 75-81.
76. Schneiera, B. (2019). "Árboles de ataque. Revista la Academia, 1(1), 1-4."
77. Serrano, Cristhian (2021). https://www.lafm.com.co/tecnologia/como-se-produjo-el-ciberataque-universidad-el-bosque-y-quienes-afecta
78. Sonnenreich W, et al (2005) Return on Security Investment (ROSI): A Practical Quantitative Model
79. Terry Ingoldsby. (2021) Attack Tree-based Threat Risk Analysis
80. Tünnermannos, C. (2003). La universidad ante los retos del siglo XXI. (1ª. ed.). Mérida, México: Ediciones de la Universidad Autónoma de Yucatán.
81. Ucedaveles T. & Morana M. (2015) "Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis". Indianápolis, Indiana, John Wiley & Sons Inc.,
82. Vargas, M. Zubieta, A. (2017). Diseño del sistema de gestión de seguridad de la información (SGSI) en la empresa T&S. Comp. Tecnología y Servicios S.A.S., en

los procesos de apoyo, misionales y estratégicos, basado en la norma ICONTEC ISO 27001:2013.

83. Villa S (2018) IMPACTO DEL RIESGO CIBERNÉTICO EN EL SEGMENTO MIPYME
84. Vivanco Muñoz, P. E., Cortez Vásquez, A., & Bustamante Olivera, V. H. (2011). La seguridad de la información. Revista De investigación De Sistemas E Informática, 8(1), 25–30. Recuperado a partir de https://revistasinvestigacion.unmsm.edu.pe/index.php/sistem/article/view/4992.
85. Voroncovs, Aleksejs. 2016. "Investigation of tool-based modeling techniques for safety and security critical systems".
86. Yanes, J. (2018). *Las TIC y la crisis de la educación algunas claves para su comprensión*. (1ª. ed.). Colombia: Editorial Biblioteca Digital Virtual Educa.
87. YAQOOB et al (2019). *Framework for Calculating Return on Security Investment (ROSI) for Security-Oriented Organizations*
88. Yépez, J., Alvarado, J., Ortiz, M. & Acosta, N. (2017). Análisis y prevención del Ransomware en la Universidad de Guayaquil. *Espirales Revista Multidisciplinaria de Investigación, 1*(11), 68 – 72.
89. Yohai, A. S. (2019). *Informe de las tendencias del cibercrimen en Colombia en Colombia (2019- 2020)*. Bogotá, Colombia: Cámara Colombiana de Informática y Telecomunicaciones CCIT.