Universidad Cenfotec

Maestría en Ciberseguridad

Documento final de Proyecto de Investigación Aplicada 2

Propuesta de instrumento de evaluación de la aplicabilidad del marco de trabajo de Cyber Kill Chain, para el establecimiento de estrategias de seguridad de la información en las organizaciones en Costa Rica

Kirton Méndez Jurguen Axel

Fecha: marzo, 2021

Declaratoria de derechos de autor

Dedicatoria y agradecimientos

Un agradecimiento especial a mi familia por el apoyo brindado a lo largo de la carrera y por mantener la motivación de culminarla.

Se agradece la participación de Luis Naranjo Zeledón quien con su gran conocimiento en temas de investigación hizo un aporte importante para asentar las bases de este proyecto, las cuales sirvieron para el desarrollo completo del mismo.

A Luis Alonso Ramírez Jiménez por su aporte como tutor de este trabajo y por los diferentes aportes que realizó para lograr dar forma a la herramienta de evaluación de aplicabilidad del marco de trabajo de Cyber Kill Chain que en este trabajo se desarrolló y que es el principal entregable.

A Alex Araya Rojas y a Ignacio Trejos Zelaya por el aporte realizado en la lectura y revisión de este trabajo de investigación y por las sugerencias que aportaron ambos durante la defensa de este proyecto.

A la universidad Cenfotec por el apoyo y la buena disposición de los recursos necesarios para el desarrollo a lo largo de la maestría.

Universidad CENFOTEC
SOMOS LO QUE SABEMOS

Universidad Cenfotec
Carrera de Postgrado
Maestría en Ciberseguridad

TRIBUNAL EXAMINADOR

Este proyecto fue aprobado por el Tribunal Examinador de la carrera: **Maestría en Ciberseguridad,** requisito para optar por el título de grado de **Maestría,** para el estudiante: **Kirton Méndez Jurguen Axel.**

Alonso Ramírez
Digitally signed by Alonso Ramírez
Date: 2022.03.08 18:30:50 -06'00'

M. Sc. Luis A. Ramírez Jiménez
Tutor

Firmado digitalmente por ALEX ARAYA ROJAS (FIRMA)
Fecha: 2022.03.11 08:20:20 -06'00'

M. Sc. Alex Araya Rojas
Lector 1

IGNACIO TREJOS ZELAYA (FIRMA)
Firmado digitalmente por IGNACIO TREJOS ZELAYA (FIRMA)
Fecha: 2022.03.11 09:16:13 -06'00'

M. Sc. Ignacio Trejos Zelaya
Lector 2

San José, Costa Rica, 04 de marzo de 2022

Firmada digitalmente, de conformidad con la Ley de Certificados, Firmas Digitales y Documentos Electrónicos N° 8454, destacando el artículo 9°.

Tabla de contenido

Abstract

A través del tiempo se han perpetrado diferentes y variados tipos de ataques cibernéticos en Costa Rica, lo que ha llevado al país a desarrollar estrategias de seguridad que ayuden a proteger los intereses del país según la protección de la información. Además de los ataques comunes que muchos expertos en seguridad de la información conocen, también se han ejecutado ataques del tipo APT, por sus siglas en inglés, o amenazas persistentes avanzadas, las cuales llegaron a ser conocidas, pero no de forma inmediata por lo que no se ha logrado responder de forma apropiada ante este tipo de ataques.

El objetivo de esta investigación es evaluar la capacidad de aplicar el marco de trabajo de Cyber Kill Chain, el cual es muy utilizado para contrarrestar las amenazas persistentes avanzadas y otros tipos de amenazas con el fin de establecer estrategias de seguridad de la información que coadyuven a la mitigación de este tipo de ataques. Para esto, se pretende evaluar el estado actual país en materia de seguridad de la información, para identificar qué se ha implementado para responder ante este tipo de ataques, o bien si se ha implementado para lograr el mismo objetivo de respuesta.

Además, se pretende comparar con otros marcos de trabajo como ATT&CK de MITRE y con el marco de trabajo actualizado Intelligence Driven Defense, con el fin de conocer que ofrecen cada uno de los marcos de trabajo y así determinar, también, si el marco de trabajo Cyber Kill Chain es adaptable, o bien verificar la posible existencia de una convergencia entre dichos marcos de trabajo, de tal manera que sirva para el establecimiento de estrategias de seguridad de la información que mejor se adapten al país.

Palabras Clave: amenaza persistente avanzada, grupos APT, ataque de día cero, Cyber Kill Chain, amenazas de nueva generación, amenazas polimórficas.

Capítulo 1. Introducción

1.1 Generalidades

Es conocido que Costa Rica ha sido víctima de amenazas persistentes avanzadas, como la que se reportó en el año 2018, donde según el informe titulado “Costa Rica fue blanco de ataques de espionaje cibernético de Corea del Norte en 2018”, se identificaron diferentes tipos de ataques que se consideraron avanzados por mostrar características y patrones evolucionados. Estos ataques se ejecutaron con fines de espionaje, los cuales a su vez se relacionaron con Corea del Norte y donde existió la posibilidad de que se llegaran a afectar instituciones bancarias, empresas e instituciones públicas del país.

Estos ataques fueron identificados por la empresa FireEye, la cual se especializa en procesos de análisis y prevención de vulnerabilidades y que ya había identificado distintos ataques que se generaron el mismo año en diferentes países, entre los cuales se encontraba Costa Rica.

Según el informe titulado “Vinculan hackers de Corea del Norte con ola de ciberataques a bancos en todo el mundo”, se asevera que un grupo de hackers de Corea del Norte estuvieron relacionados con estos ataques y que la mayoría de los ataques fueron dirigidos a entidades financieras, donde incluso provocaron pérdidas de “cientos de millones de dólares”. Cabe señalar, que se identifica principalmente al grupo APT38 como los responsables directos; sin embargo, es conocido que este grupo puede pertenecer a un grupo principal llamado “Lázaro”; no obstante, estos se especializan en obtener fondos para el régimen de Kim Jong-un, a través del uso de habilidades particulares y contando con el uso de herramientas sofisticadas.

Según el informe titulado “Costa Rica fue blanco de ataques de espionaje cibernético de Corea Del Norte en 2018” se especifica que la compañía FireEye logró detectar diferentes tipos de acciones anómalas, que se identificaron como amenazas persistentes avanzadas y las cuales fueron detectadas a través del uso de sensores distribuidos que esta compañía tiene ubicados en algunos de sus clientes.

También, se establece que el reporte de Forey que en el país, en realidad, se habían detectado los grupos APT37 y APT38, el primero se especializa en la identificación de vulnerabilidades no conocidas por los softwares antivirus y el otro solo mantiene interés en el sector financiero.

Además, según el informe titulado “Vinculan hackers de Corea del Norte con ola de ciberataques a bancos en todo el mundo”, a lo largo del tiempo se han detectado distintos ataques elaborados por el grupo APT38. La nota internacional informa sobre incidentes relacionados que se habían estado ejecutando desde el año 2014, donde este grupo ya había logrado vulnerar a una gran cantidad de instituciones financieras de distintos países a través del uso de técnicas sofisticadas, utilizando identificaciones falsas y utilizando técnicas específicas como el phishing.

Según el informe titulado “Costa Rica fue blanco de ataques de espionaje cibernético de Corea del Norte en 2018” se le había consultado a Roberto Lemaitre sobre si el Gobierno de la República había logrado percibir una amenaza persistente avanzada, a lo que el experto aseguró:

> Es difícil detectar un APT. Es bastante complejo. ¿Por qué? Porque buscan aprovecharse de los recursos a través de vulnerabilidad sin que se den cuenta. Por ejemplo, usan firmas de ataques únicas, que entonces tampoco las van a detectar muchos de los sistemas. Aprovechan esas firmas, principalmente, para no ser detectados y estar periodos largos de tiempo sin que los encuentren. Y entonces los ataques vienen desde una gran variedad de fuentes. Eso hace más complejo el ataque. Es muy complejo lograr determinarlos, entonces por eso es difícil detectarlos.

Por esta razón, cabe señalar que las autoridades nacionales y muchas instituciones no estaban preparadas en aquel momento, porque no lo habían detectado y además porque en sí la particular complejidad de estos ataques hace que aun hoy en día sea complejo detectarlos. Además, de la complejidad existente para detectar con precisión este tipo de ataques, existe el gran impacto que produce a la población, en donde existen pérdidas financieras importantes.

1.2 Antecedentes del problema

En los últimos años se han presentado a nivel mundial múltiples ataques, los cuales han generado pérdidas económicas importantes, incluso han atentado contra vidas humanas, especialmente aquellos que dirigen infraestructuras críticas. Según el Estudio Global de Ciberseguridad 2018 (GCI por sus siglas en inglés) y con base en la figura 1, se demuestra que Costa Rica se encuentra en la posición 115 con

respecto a 173 países que forman parte de este ranking a nivel mundial y en el puesto 18 respecto al continente americano.

Member State	Score	Regional Rank	Global Rank
Peru	0.401	12	95
Panama	0.369	13	97
Ecuador	0.367	14	98
Venezuela	0.354	15	99
Guatemala	0.251	16	112
Antigua and Barbuda	0.247	17	113
Costa Rica*	0.221	18	115
Trinidad and Tobago	0.188	19	123
Barbados	0.173	20	127
Saint Vincent and the Grenadines	0.169	21	129
Bahamas	0.147	22	133
Grenada	0.143	23	134
Bolivia (Plurinational State of)	0.139	24	135
Guyana	0.132	25	138
Nicaragua	0.129	26	140
Belize	0.129	26	140
El Salvador*	0.124	27	142
Suriname	0.110	28	144
Saint Lucia	0.096	29	149
Saint Kitts and Nevis	0.065	30	157
Haiti	0.046	31	164
Honduras	0.044	32	165
Dominica	0.019	33	172

Figura 1: Ranking global y regional. Fuente: Estudio Global de Ciberseguridad 2018.

Además de la baja calificación a nivel global, la figura 2 muestra que Costa Rica tiene un bajo nivel de compromiso con la ciberseguridad, lo cual demuestra a su vez la razón de porqué el país se ha visto vulnerable ante diferentes tipos de ataques, donde se incluyen las amenazas persistentes avanzadas.

Low		
Gabon	Afghanistan	Mali
State of Palestine	Barbados	Timor-Leste
Senegal	Myanmar	San Marino
Sudan	Saint Vincent and the	Marshall Islands
Gambia	Grenadines	Somalia
Ethiopia	Congo	South Sudan
Malawi	Cambodia	Saint Kitts and Nevis
Tajikistan	Mozambique	Sao Tome and Principe
Iraq	Bahamas	Djibouti
Algeria	Grenada	Solomon Islands
Nepal	Bolivia	Tuvalu
Seychelles	Sierra Leone	Guinea-Bissau
Kyrgyzstan	Eswatini	Cabo Verde
Guatemala	Guyana	Lesotho
Antigua and Barbuda	Papua New Guinea	Haiti
Syrian Arab Republic	Nicaragua	Honduras
Costa Rica	Belize	Micronesia
Tonga	Namibia	Central African Republic
Libya	El Salvador	Equatorial Guinea
Liberia	Turkmenistan	Kiribati
Bosnia and Herzegovina	Andorra	Vatican
Madagascar	Suriname	Eritrea
Lao	Mauritania	Democratic People's Republic
Fiji	Nauru	of Korea
Guinea	Chad	Dominica
Trinidad and Tobago	Vanuatu	Yemen
Zimbabwe	Angola	Comoros
Lebanon	Saint Lucia	Democratic Republic of the
Bhutan	Niger	Congo
	Burundi	Maldives
	Togo	

Figura 2: Bajo nivel de compromiso con la ciberseguridad. Fuente: Estudio Global de Ciberseguridad 2018. Fuente: Estudio Global de Ciberseguridad 2018.

Según el informe titulado “Costa Rica recibió 19 millones de ciberataques durante primer trimestre: sector público no está preparado”, se menciona que el país cuenta con el centro de Respuesta de Incidentes de Informática (CSIRT-CR), el cual se encarga de monitorear incidentes de ataques y además provee ayuda a instituciones afectadas. Sin embargo, en la misma nota el experto Roberto Lemaitre menciona:

> A nivel país hemos hecho los análisis de vulnerabilidades del sector público que nos permitan evaluarlas y darles un plan de remediación para disminuir la posibilidad de que un incidente las afecte, la idea es prevenir, pero siempre va a haber un nivel de vulnerabilidad, hay temas que corregir y trabajar, pero estamos tratando de disminuir las vulnerabilidades al mínimo; hay temas que mejorar.

También, se menciona que muchos de los ataques específicos que afectan al país son del tipo ramsonware, phishing y malware. Incluso, Roberto Lemaitre menciona “… el tiempo de respuesta es de 24 horas para reestablecer los servicios”. Según el informe titulado “Costa Rica recibió 19 millones de ciberataques durante primer trimestre: sector público no está preparado”, otra problemática es que existe muy poco conocimiento por parte de las personas y no existe una cultura digital que coadyuve a prevenir sobre ciertos riesgos o amenazas a nivel de seguridad de la información. Se han realizado esfuerzos para disminuir estos riesgos como la capacitación de las personas; sin embargo, es un problema que normalmente tiende a perdurar a lo largo del tiempo.

Es importante señalar que el país no ha sido únicamente afectado por ataques APT, normalmente han estado ocurriendo ataques a nivel nacional que han tenido un fuerte impacto económico sobre distintas instituciones del país. Como menciona en el informe titulado “Costa Rica recibió 19 millones de ciberataques durante primer trimestre: sector público no está preparado” hubo ataques que afectaron específicamente al Poder Judicial, el 6 de febrero; el Archivo Nacional, el 18 de febrero; la Cancillería, el 14 de marzo; la Asamblea Legislativa, el 25 de marzo y el Consejo de Seguridad Vial (Cosevi), el 22 de abril, todos ocurrieron en el año 2019.

Como efecto directo de estos ataques, hubo afectaciones a nivel de los servicios públicos del país, por lo que de igual manera tuvieron un impacto considerable. A pesar de que se logró dar respuesta ante estos incidentes, no se

lograron evitar o mitigar con mayor precisión, lo cual demuestra que a pesar de los esfuerzos que se han venido realizando, incluso para evitar o mitigar ataques APT, el país ha mostrado ser muy vulnerable ante diferentes tipos de ataques. Se considera el hecho de que en el año 2018 ya se había experimentado un APT y aun así, el país siguió mostrando ser vulnerable para el año 2019, lo cual demuestra claramente que a pesar de los esfuerzos realizados, el país no ha logrado un alto nivel en materia de seguridad de la información.

Incluso, según el informe titulado “Costa Rica recibió 19 millones de ciberataques durante primer trimestre: sector público no está preparado”, se menciona otra lista de instituciones que fueron afectadas en años anteriores como las municipalidades de Matina, Corredores y Puntarenas en el año 2018, el Ministerio de Trabajo, en el 2014; la Comisión Nacional para el Adulto Mayor (Conapam), en el 2015 y 2018; el Instituto Costarricense de Ferrocarriles (Incofer), en el 2015 y el Ministerio de Ambiente y Energía (Minae), en el 2016. Dentro de las amenazas que se han identificado se encuentran ataques ramsonware, de fuerza bruta y los de denegación de servicios.

Según señala el informe titulado “Costa Rica recibió 19 millones de ciberataques durante primer trimestre: sector público no está preparado”, muchos de los ataques ocurridos tienen su origen en el continente asiático; sin embargo, se señala específicamente a países como Corea del Norte y a Pakistán como las principales naciones encargadas de ejecutar la mayoría de los ataques hacia Costa Rica. En el caso de Corea del Norte se conoce el incidente ocurrido en el año 2018 con ataques APT y el caso de Pakistán, donde un grupo de hackers de esa misma nación, conocidos como Pak Monster, se habían atribuido diferentes ataques sucedidos a sitios web gubernamentales y que habían tenido afectación en los dominios con extensión .go.cr.

1.3 Definición y descripción del problema

Actualmente, en relación con lo sucedido a nivel global, en Costa Rica se ha observado de forma recurrente, que las organizaciones en el país no se encuentran preparadas para atender de forma efectiva los ataques cibernéticos que se han

estado perpetuando desde años anteriores, así como los que eventualmente podrían llegar a ocurrir más adelante.

Con base en el reporte de “Ciberseguridad 2020 sobre riesgos, avances y el camino a seguir en América Latina y el Caribe”, se establece que el país ha venido realizando diferentes esfuerzos con el fin de reforzar la seguridad de la información a nivel nacional. Como parte de estos esfuerzos, el mismo reporte señala que en el año 2017 se estableció la Estrategia de Seguridad Nacional de Ciberseguridad por parte del Ministerio de Ciencia, Tecnología y Telecomunicaciones (Miciit), y en el 2012 se creó el CSIRT-CR, a partir del decreto Decreto Nº 37.052 bajo la misma institución. En ese mismo año, se estableció el Decreto Legislativo Nº 9.048, por el cual se establecieron disposiciones para el delito cibernético.

Además, el reporte menciona que Costa Rica es parte del convenio de Budapest, así como también de otros convenios que están relacionados con la estrategia de ciberseguridad que ha ido implementándose en el país. También se estableció la Ley Nº 8.968 de Protección de la persona frente al tratamiento de sus datos personales con el fin de proteger los datos personales de la población costarricense.

A pesar de esto, se ha logrado demostrar que en Costa Rica las organizaciones no se encuentran preparadas para atender ataques cibernéticos de forma adecuada, a pesar de que se han desarrollado diferentes mecanismos con el fin de mitigar o evitar estos ataques. Al considerar la complejidad de las amenazas persistentes avanzadas, es muy importante considerar diferentes aspectos de manera más puntual, para una mayor comprensión del problema, por lo que en la figura 3 se demuestra que Costa Rica a nivel de política y estrategia de seguridad cibernética muestra niveles bajos de cumplimiento; sin embargo, lo que más destaca es que la respuesta a incidentes, a pesar de ser baja, la protección de la infraestructura crítica (IC) y la defensa cibernética son unos puntos más vulnerables al mostrar los niveles más bajos. Estos aspectos son importantes a considerar dado que, ante una amenaza persistente avanzada, el país no cuenta estos aspectos importantes para la mitigación o respuesta ante este tipo de incidentes.

Figura 3: Política y Estrategia de Seguridad Cibernética. Fuente: Reporte de Ciberseguridad 2020 sobre Riesgos Avances y el camino a seguir en América Latina y el Caribe.

También, en la figura 4 se demuestra que el país mantiene bajos niveles con respecto al apartado relacionado a los estándares, las organizaciones y las tecnologías, en todos los aspectos que lo comprenden. Cabe señalar que, de cada uno de los aspectos mencionados en este apartado, algunos tienen relación directa con los APT, mientras que otros mantienen una relación indirecta con los APT.

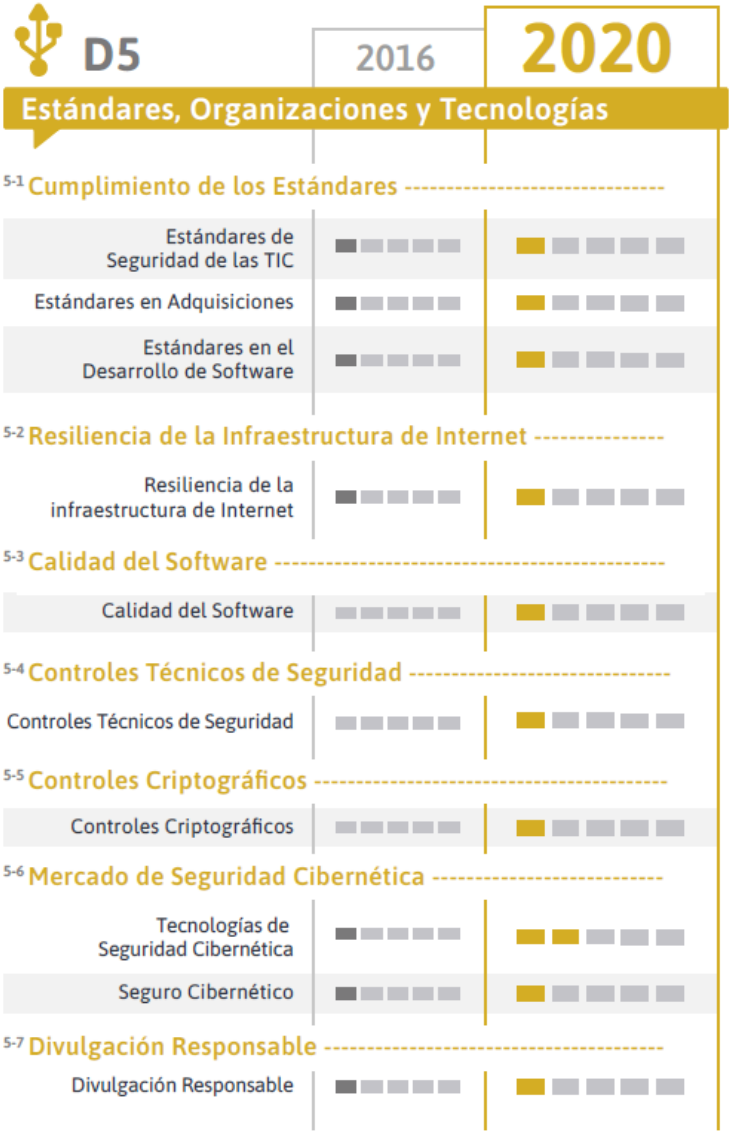


Figura 4: Estándares, Organizaciones y Tecnologías. Fuente: Reporte de Ciberseguridad 2020 sobre Riesgos Avances y el camino a seguir en América Latina y el Caribe.

Considerando los aspectos mencionados anteriormente, se establece que el presente trabajo tiene como objetivo evaluar la capacidad de aplicar el marco de trabajo de Cyber Kill Chain, para determinar estrategias de seguridad que permitan contrarrestar, mitigar o al menos responder ante amenazas persistentes avanzadas en Costa Rica. De tal manera, que se logre mejorar los diferentes niveles de seguridad que necesitan una mayor atención y que a su vez se ven directa o indirectamente impactados por ataques APT.

Se destaca que el marco de trabajo propuesto es altamente aplicable a este tipo de amenazas en donde incluso existen otros marcos de trabajo comparables, los cuales también deberán de ser evaluados para definir una estrategia de seguridad de la información más exacta y aplicable al contexto y necesidades reales del país.
La propuesta se establece a partir de conocer que en años recientes Costa Rica fue afectada por amenazas persistentes avanzadas provenientes de diferentes países con intereses distintos, pero con el mismo objetivo.

1.4 Justificación

A pesar de que el país está haciendo esfuerzos para atender los desafíos de ciberseguridad que presentan las nuevas amenazas persistentes avanzadas en el mundo es importante contar con una propuesta de evaluación de aplicabilidad del marco de trabajo de Cyber Kill Chain, para el establecimiento de estrategias de seguridad para la información en Costa Rica, con el fin de ayudar a las organizaciones en Costa Rica del sector público y privado a que no pierdan inversión o recurso financiero por ser víctimas de robo o pérdida de datos, secuestro de información, alteración de información o no disponibilidad de sus servicios o infraestructuras críticas o tecnológicas. Además de esto, se visto un gran impacto en la disponibilidad de los servicios públicos del país, por lo cual también es importante contar con una propuesta de tal índole.

Además, es importante resolver el problema de las APTs en Costa Rica, pues hoy podemos ver que organizaciones del sector público y privado, en caso de que sean víctimas de un ataque, pueden ver comprometidos sus servicios u operaciones. En el caso del sector público si se afectan los servicios, no van a haber servicios críticos disponibles a la ciudadanía para continuar sus acciones del día, por lo cual tiene un alto impacto a nivel de la población, en especial si se interrumpen servicios de salud, los cuales ahora son los más críticos. Además, si el sector privado se ve afectado, existirán pérdidas financieras que van a significar la reducción del costo o del gasto a través de dejar de prescindir de personal humano o al dejar de invertir en nuevas fuentes de trabajo, lo cual tiene impacto directo con la generación de empleo, aspecto a considerar, dado que es lo que más está afectando al país en la actualmente.

Esta propuesta es importante, pues vendría siendo parte de una solución integral con lo que el país ha venido trabajando desde años anteriores para el reforzamiento de la seguridad de la información. Es importante considerar que hoy se requiere contar con elementos que propicien a una verdadera protección, tanto para las organizaciones públicas como las privadas dado que las mismas pueden llegar a ser víctimas de ataques APT de índole global. Con la implementación de esta propuesta se pretende buscar una solución que beneficie a la mayoría de las organizaciones y ciudadanos de todo el país.

1.5 Viabilidad

Como se ha mencionado, según el estudio del 2020 de la Organización de Estados Americanos, Costa Rica ha realizado muchos esfuerzos con el fin de mitigar o evitar los ataques cibernéticos que se han estado ejecutando desde años anteriores. Esto ha demostrado que no solo el país ha estado tratando de reforzar la seguridad de la información, sino que también ha tenido que invertir altas sumas de dinero para mejorar el estado de la seguridad en el país. Esto implica que además de las pérdidas económicas que se han visto plasmadas por los mismos ataques, se considera también los costos relacionados a evitar los mismos. Por lo cual, la propuesta que se plantea podría, eventualmente, lograr que el país mejore su estado de seguridad, pues al ser un proyecto que no implica costes ni directos ni indirectos a los diferentes interesados, entre los cuales se encontraría la población misma, así como las diferentes instituciones tanto públicas como privadas.

Asimismo, tras haber identificado todas las pérdidas millonarias que han dejado los diferentes tipos de ataques que se han perpetuado, se logra identificar a su vez un beneficio importante del presente proyecto, pues con la implementación de la propuesta que se estaría estableciendo, se lograría reducir en gran medida la cantidad de ataques que afectan al país, incluso, el beneficio económico se vería reflejado al ver que el mismo proyecto podría aplicarse sobre otro tipo de amenazas y no solamente sobre amenazas persistentes avanzadas.

Con lo anterior, el país también se ve beneficiado, dado que contribuye para el cumplimiento sobre ciertas normas o políticas internacionales, las cuales podrían afectar, ya sea la imagen del país o la aplicación de normas que conllevarían a multas por la desprotección de datos o información de interés nacional e internacional. Como

parte de lo anterior, cabe señalar que el país es actual miembro de la Organización para la Cooperación y el Desarrollo Económicos (OCDE), por lo cual, al reforzar la estrategia de seguridad del país, el proyecto logra ser viable al demostrar que refuerza su estado de seguridad, lo que a su vez representaría una mejor imagen para el país a nivel internacional, dado que se lograría demostrar la competencia ante situaciones de ataques avanzados cibernéticos.

1.5.1 Punto de vista técnico

Como parte de la maestría en ciberseguridad, el autor cuenta con conocimiento idóneo para el desarrollo de la investigación, dado que a lo largo de la carrera se han adquirido los conocimientos, la experiencia y las competencias suficientes como para aplicar un proceso de investigación relacionada con la ciberseguridad. Como parte de demostrar capacidad técnica, el investigador ha desarrollado diferentes tipos de tareas relacionadas con la ejecución de ataques cibernéticos en ambientes controlados, en los que también ha tenido la oportunidad de realizar diferentes tipos de pruebas de penetración.

1.5.2 Punto de vista operativo

Al considerarse que la investigación se aplica a nivel nacional y considerándose que la información tanto de medios de comunicación como de otros medios confiables de información son gratuitos y abiertos a compartir información existe la posibilidad de realizar la investigación de tal manera que se logre aplicar con información totalmente confiable y exacta.

1.5.3 Punto de vista económico

Al considerarse que el proyecto se aplica a nivel país y los resultados de este están orientados a que sea una contribución que ayude al país de tal manera que se realice un aporte en materia de seguridad de la información, los gastos asociados a electricidad, licencias de software, hardware, entre otros corren por cuenta del autor del proyecto.

1.6 Objetivos

Se utiliza la taxonomía de Bloom de 1956, dado que es la más utilizada en el país en el ámbito de la investigación y además, porque permite definir los objetivos con una estructura ordenada que permite al lector conocer de forma inmediata qué se va a realizar durante el proceso de la investigación.

1.6.1 Objetivo general

Proponer un instrumento de evaluación de la aplicabilidad del marco de trabajo Cyber Kill Chain, para el establecimiento de estrategias de seguridad de la información en las organizaciones en Costa Rica.

1.6.2 Objetivos específicos

- Identificar las estrategias de seguridad de la información que se hayan implementado en el país, por medio del estudio de las diferentes leyes, políticas y estándares del país para identificar áreas de mejora.
- Comprender las estrategias implementadas en el país, a través del análisis de la información obtenida, para definir el contexto sobre el cual se analizará el marco de trabajo.
- Desarrollar un proceso de investigación a través de la recolección de información, por medio una encuesta para obtener información más precisa sobre el uso y la aplicabilidad del marco de trabajo de Cyber Kill Chain.
- Analizar el marco de trabajo de Cyber Kill Chain, a través de su propio estudio, para definir su aplicabilidad en el contexto del país.

1.7 Alcances y limitaciones

1.7.1 Alcances

Documento escrito de la investigación que incluye el instrumento de evaluación de la aplicabilidad del marco de trabajo de Cyber Kill Chain, para establecer estrategias de seguridad.

1.7.2 Limitaciones.

No se considera aplicar o dirigir la investigación para producir un resultado a nivel internacional, solo nacional.

La aplicabilidad de la investigación se limita a recursos gratuitos, por lo que no se considerarán documentos o investigaciones que involucren costos para el desarrollo de la investigación.

1.8 Marco de referencia organizacional y socioeconómico

Costa Rica es un país en democracia que tiene una población de aproximadamente 5 millones con un estimado de 333,980 personas viviendo en su capital San José.

El estado soberano es una república constitucional presidencial unitaria. Es conocido por su democracia estable y duradera, y por su fuerza laboral altamente educada, la mayoría de los cuales habla inglés.

Su economía, una vez fuertemente dependiente de la agricultura, se ha diversificado para incluir sectores como finanzas, servicios corporativos para empresas extranjeras, productos farmacéuticos y ecoturismo. Muchas empresas extranjeras de fabricación y servicios operan en las Zonas Francas de Costa Rica, donde se benefician de incentivos fiscales y a la inversión.

El país ha tenido un desempeño consistentemente favorable en el índice de desarrollo humano, ubicándose en el puesto 62 en el mundo a partir de 2020 y en el quinto en América Latina. También, ha sido citado por el Programa de las Naciones Unidas para el Desarrollo, por haber alcanzado un desarrollo humano mucho más alto que otros países con el mismo nivel de ingreso, con un mejor historial de desarrollo humano y desigualdad que la mediana de la región.

En materia de seguridad de la información, Costa Rica ha logrado el desarrollo de múltiples estrategias orientadas a la mejora de la protección de la información. Entre ellas se encuentran las siguientes:

- En el año 1971 se estableció la Ley No. 4755 Modificación del Código de Normas y Procedimientos Tributarios con reformas en los artículos 94 al 97.
- En el año 1995 se estableció la Ley No. 7557 Ley General de Aduanas sobre la cual se han hecho reformas en los artículos del 219 al 223.

- En el año 1997 se había creado la sección de Delitos Informáticos, la cual forma parte de la Unidad de Investigación Informática del Departamento de Investigaciones Criminales del Ministerio Público.
- En el año 2001 Costa Rica se adhirió al convenio de Budapest, por medio de la Asamblea Legislativa.
- En el año 2010 se estableció un borrador para el desarrollo de una estrategia basada en un gobierno electrónico, la cual se estableció con el fin de ofrecer servicios digitales que estuvieran más orientados a los ciudadanos del país.
- En el mismo año se establece la Comisión Nacional de Seguridad en Línea (CNSL), la cual se encarga de definir las políticas para un correcto uso del Internet y las Tecnologías Digitales.
- En el año 2011 se aprobó y publicó por medio del diario *La Gaceta* N.170 la Ley Nº 8.968 de Protección de la Persona frente al tratamiento de sus datos personales, con el fin de fortalecer la privacidad y la protección de los datos personales de los ciudadanos costarricenses.
- En el año 2012 se aprobó el Decreto Legislativo Nº 9.048, con el fin de plantear una reforma al Código Penal, de tal manera que se lograran incluir disposiciones para el delito cibernético.
- También en el mismo año se creó un CSIRT nacional (CSIRT-CR) bajo el Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT), por medio del Decreto Nº 37.052, el cual hasta hoy se mantiene gestionado por la Dirección de Gobernanza Digital del MICITT. El CSIRT es miembro del CSIRT de las Américas.
- En el año 2017 el MICITT estableció la Estrategia Nacional de Ciberseguridad, la cual define la infraestructura crítica en términos de “sistemas de información y redes, que en caso de falla podrían tener un impacto serio en la salud, la seguridad física y operativa, la economía y el bienestar de los ciudadanos. Este documento se había comenzado a discutir desde el mes de mayo del 2015 y para el mes de junio del 2017 se sometió a Consulta Pública no vinculante por medio de la publicación de este a través del diario oficial *La Gaceta* N. 105.
- En el presente año Costa Rica volvió a adherirse al Convenio de Budapest y también se adhirió a otros convenios de importancia para el fortalecimiento de la estrategia de seguridad de la información. Con esta adhesión el país logró

ser un hub de la Acción Mundial contra los Delitos Cibernéticos Extendido (GLACY+).

- En el año 2018 se presentó el proyecto de ley N.º 21187 Ley para Combatir la Ciberdelincuencia, con el fin de adecuar el marco penal a lo que exige el convenio de Budapest.

1.9 Estado de la cuestión

Actualmente, muchas organizaciones a nivel mundial están aplicando diferentes estrategias para la mitigación de ataques APT en todos los ámbitos y aplicando diferentes métodos que mejor se adapten a este tipo de ataques, entre los cuales está la metodología Cyber Kill Chain, la cual a pesar de que es algo reciente, existen investigaciones relacionadas a la aplicación de esta metodología, así como documentación generada por la misma empresa encargada de desarrollar dicha metodología. Por lo tanto, se pretende recopilar diferentes tipos de documentos, tanto investigación aplicada por terceros, como documentación oficial de la empresa dueña de la metodología que sea relevante, con el fin de desarrollar la investigación con base a la identificación, selección y análisis de dicha documentación.

1.9.1 Planificación de la revisión

En esta sección se formulará una pregunta clara y definida del tema de investigación. Para esto, se procederá a la revisión sistemática desde diferentes fuentes, donde se identifique documentación existente con el objetivo de comprender qué se ha desarrollado a nivel académico relacionado con el tema que será investigado, con el fin de reconocer que no haya duplicidad sobre los estudios que han realizado en otras investigaciones.

1.9.1.1 Formulación de la pregunta

Se formula una pregunta con la cual se pretende reducir el proceso de búsqueda de información que servirá de base para la investigación, con el fin de demostrar la validez de este trabajo y relacionar ideas, conceptos, teorías, así como la implementación práctica de los mismos.

1.9.1.1.1 Foco de la pregunta

Dada la naturaleza de este trabajo de investigación se pretende centralizar la búsqueda de documentos, tanto técnicos como no técnicos, en los que se demuestre el uso y la efectiva implementación de la metodología Cyber Kill Chain, para amenazas APT.

1.9.1.1.2 Amplitud y calidad de la pregunta

Considerando los puntos anteriores, se establece una pregunta clara y concisa con el fin de resolver el problema planteado. Por lo cual, se deben definir diferentes puntos que coadyuven a la definición del contexto sobre el cual se realizará la investigación y que a su vez ayude a responder de manera efectiva la pregunta planteada. Para esto, se define una serie de términos o conceptos que se identifican como principales y que sean de relevancia para aplicar el proceso de búsqueda de información, por lo que a continuación se consideran algunos puntos importantes:

1. Problema. El avance de la tecnología y la digitalización acelerada sobre diferentes procesos que son básicos para llevar a cabo diferentes tareas la vida diaria ha conllevado a una mayor exposición de la información generando un aumento en los ataques cibernéticos. Dado que parte de estos procesos se administra información que puede de carácter confidencial, a pesar de que se implementan mecanismos de seguridad sofisticados, también existen grupos encargados de llevar a cabo ataques que también son altamente sofisticados, los cuales evaden muchos de los mecanismos conocidos de seguridad para la protección de la información.

Normalmente la ejecución de estos ataques es catalogada como ataques APT (Advanced Persistent Threats), los cuales afectan de distintas formas a diferentes países, empresas y personas a nivel mundial. Sin embargo, su impacto es alto debido a que normalmente se llega a comprometer información confidencial y muy delicada que incluso puede llegar a afectar en gran medida a quienes son víctimas de ellos. Así como han evolucionado estos ataques, han aparecido diferentes metodologías y mecanismos para contrarrestar su impacto como lo es la metodología Cyber Kill Chain, la cual en la práctica ha demostrado ser efectiva para estos tipos de ataques.

La presente investigación se orienta al estudio de la metodología Cyber Kill Chain para establecer una estrategia de seguridad de la información frente a ataques APT.

2. Pregunta. Con base al problema anteriormente identificado, se plantea la siguiente pregunta de investigación: ¿Qué investigaciones se han desarrollado relacionadas a la aplicación de la metodología Cyber Kill Chain, para mitigar ataques APT?
3. Palabras claves y sinónimos. A continuación, en la tabla 1 se presenta un listado de palabras clave, las cuales van a ser ampliamente utilizadas para realizar el proceso de búsqueda de información relevante publicada en diferentes tipos de documentos, así como trabajos que tengan relación con la investigación. Dado que la mayoría de los documentos están en el idioma inglés, se muestra su forma traducida. Cabe señalar, que a pesar de que la mayoría de las palabras tienen traducción, algunas se van a mantener en el idioma original (inglés), dado que su uso está extendido en el ámbito profesional de la carrera y a su vez, porque son anglicismos ampliamente utilizados y aceptados por la naturaleza del área de estudio.

Tabla 1: *Listado de palabras*

Palabra clave	Traducción al inglés
Cadena de eliminación cibernética	Cyber Kill Chain
Amenaza Persistente Avanzada	Advanced Persistent Threat
Seguridad de la información	Information Security
Piratería informática	Hacking
Amenaza	Threat
Detección	Detection
Inteligencia	Intelligence
Ataques	Attacks
Espionaje	Espionage

Fuente: Elaboración propia.

4. Intervención. Ver la utilidad y efectividad de la metodología de Cyber Kill Chain para amenazas o ataques APT.

   Obtener los documentos que se identifiquen como relevantes para la investigación para analizar los resultados que se hayan obtenido.
5. Control. Se establece iniciar el proceso de investigación con el uso de palabras clave anteriormente definidas.

6. Efectos. Se espera concebir la documentación necesaria que tenga información sustancial con base al proceso de búsqueda aplicado para comprender cómo la metodología de Cyber Kill Chain puede ser útil para la mitigación de amenazas APT y tener un mayor conocimiento sobre los esfuerzos realizados en Costa Rica relacionado a este campo.
7. Medida de salida. Se pretende utilizar fuentes basadas en sitios web para identificar la idoneidad de la revisión de calidad que se debe de aplicar a los distintos documentos encontrados.
8. Población. La población para que se verá beneficiada con esta investigación será la población costarricense.
9. Aplicación. Esta investigación puede llegar a ser de gran interés para las personas dada su naturaleza de gran alcance al abarcar la seguridad de la información que es de interés general. Además, de manera más específica puede ser de gran interés para profesionales en informática, así como para otros tipos de profesionales que deseen obtener o extender su conocimiento en el ámbito de la seguridad de la información.
10. Diseño experimental. Para el diseño experimental se aplica un proceso de análisis y de clasificación minucioso de las investigaciones obtenidas considerándose aspectos como la calidad y la importancia que los mismos tengan para la investigación. Esto con el fin de dar garantía de que la documentación tiene concordancia con la investigación y que la cantidad de documentos utilizados sea la idónea, para un rango aceptable de estudios o investigaciones para el desarrollo de una investigación más precisa.

1.9.1.2 Selección de fuentes

Se definen las fuentes a utilizar para identificar estudios primarios que servirán para comenzar la investigación.

1.9.1.2.1 Definición del criterio de selección de fuentes

Para el proceso de selección de fuentes, se han definido varios aspectos de selección, entre los cuales se considera el prestigio de los investigadores y de sus respectivos trabajos de investigación. Sin embargo, dado que el tema de Cyber Kill Chain es en parte muy reciente, a pesar de que existen varias investigaciones y documentación al respecto, muchas de estas no han pasado por un proceso formal

de revisión, por lo cual puede que existan documentos de investigaciones, así como documentos proveídos por la misma empresa que desarrolló la metodología que no estén verificados o avalados, pero que son de alta importancia para el desarrollo de este trabajo de investigación.

1.9.1.2.2 Lenguaje de estudio

Para aplicar el estudio en cuestión se definen los idiomas inglés y español para lograr contar con un mayor rango de documentación disponible para dicha investigación.

1.9.1.2.3 Identificación de fuentes

Se define la descripción de la selección de fuentes para identificar la forma en cómo será ejecutada la búsqueda y se define una lista de fuentes seleccionadas. A continuación, se muestra el proceso para la selección de fuentes:

1. Método de selección de fuentes. En el método de selección de fuentes se definen las diferentes fuentes a utilizar en la investigación con base al respaldo y prestigio de cada una de las publicaciones de estudios y de documentos investigativos. También, se considera la facilidad para realizar búsquedas y consultas en los diferentes medios de búsqueda.
2. Cadena de búsqueda. A continuación, se describen las cadenas de búsqueda a utilizar basado en la combinación “AND” y “OR”:
   ("Cyber Kill Chain" AND ("information security" OR "Advanced Persistent Threats" OR "hacking" OR “threat” OR "detection" OR "intelligence" OR "attacks" OR espionage)) OR ("Seguridad de la información" AND "cyber kill chain") OR ("Amenazas Persistentes Avanzadas" AND "Cyber Kill Chain") OR ("Ataques" AND "Cyber Kill Chain") OR ("Advanced Persistent Threats" AND ("information security" OR "hacking" OR “threat” OR "detection" OR "intelligence" OR "attacks" OR "espionage")) OR ("Amenaza Persistente Avanzada" AND ("seguridad de la información" OR “amenaza” OR "detección" OR "Inteligencia" OR "ataques" OR "Espionaje"))
3. Lista de fuentes:
   1. Heliyon.
   2. Computers & Security.
   3. IEEE.

4. Research Gate.

1.9.1.2.4 Selección de fuentes después de la evaluación

Para la selección de fuentes después de la evaluación aplicada, se establece el proceso en donde se pretende evaluar los elementos que forman parte de la lista de fuentes inicial, con base al criterio de selección de las fuentes.

1.9.1.2.5 Comprobación de las fuentes

Para la comprobación de las fuentes, no se cuenta con un experto en el área que pueda brindar realimentación sobre las fuentes seleccionadas; sin embargo, como punto de partida para la aplicación del proceso de selección de fuentes se utilizaron diferentes herramientas y mecanismos para comprobar en la medida de lo posible que las fuentes tuviesen respaldo académico y para la documentación que no cuenta con este tipo de revisión o respaldo, dado que existen documentos muy recientes como para ser corroborados en su totalidad, se estableció la escogencia de los mismos con base a las necesidades del trabajo de investigación y teniendo en cuenta que sea información que eventualmente demuestre que las investigaciones desarrolladas son realistas y útiles en el ámbito de la investigación. Eventualmente, se espera obtener realimentación de un experto para mejorar la lista en caso de ser necesario.

1.9.1.3 Selección de estudios

Según las fuentes que se han definido, se establece cuáles documentos obtenidos de las búsquedas van a ser incluidos en el análisis.

1.9.1.3.1 Definición del criterio de inclusión y exclusión de estudios

Se establecen los criterios de inclusión y exclusión de estudios en la tabla 2. Los documentos en los que se identifiquen que cumplen con los requerimientos de inclusión son los que se considerarán.

Tabla 2: *Criterio de inclusión y exclusión de estudios*

Pregunta de investigación	Términos para el criterio de inclusión	Consideraciones para los criterios de exclusión
¿Qué investigaciones se han desarrollado relacionado a la aplicación de la metodología Cyber Kill Chain para mitigar ataques APT?	"Cyber Kill Chain", "Advanced Persistent Threat", "Amenaza Persistente Avanzada", "Information security", "Seguridad de la información", "Hacking", "Threat", "Amenaza", "Detection", "Detección", "Intelligence", "Inteligencia"	Documentos referentes a Cyber Kill Chain que no estén relacionados con su aplicación sobre amenazas persistentes avanzadas.
		Documentos referentes a Advanced Persistent Threats o Amenazas Peristentes Avanzadas que no estén relacionados a su mitigación o bien estudios técnicos específicos aplicados sobre tecnologías o herramientas específicas.
		Estudios sobre metodologías relacionadas a Cyber Kill Chain o bien la aplicación de Cyber Kill Chain en conjunto con otras metodologías.

Fuente: Elaboración propia.

1.9.1.3.2 Definición de tipos de estudio

Para la definición de tipos de estudio se considera la pregunta planteada en la investigación. A continuación, en la tabla 3 como parte de los tipos de estudio, se

presentan los requerimientos para establecer los artículos o documentación de interés.

Tabla 3: *Tipos de estudio*

Pregunta de investigación	¿Quién?	¿Qué?	¿Cómo?	¿Dónde?
¿Qué investigaciones se han desarrollado relacionado a la aplicación de la metodología Cyber Kill Chain para mitigar ataques APT?	Sistemas de información utilizados por los usuarios.	Cyber Kill Chain, Advanced Persistent Threats.	Detección, Mitigación.	Ámbito general de sistemas de información.

Fuente: Elaboración propia.

1.9.1.3.3 Procedimiento para la selección de los estudios

Se aplicó un procedimiento repetitivo para cada una de las fuentes identificadas para seleccionar estudios relevantes:

1. Aplicar la búsqueda general en cada una de las herramientas de búsqueda disponibles.
2. Con base a los resultados definidos, se aplicaron las cadenas de búsqueda establecidas para considerar aquella documentación relevante con base a los criterios de inclusión.
3. Se aplican filtros de búsqueda avanzada considerándose 5 años anteriores al presente para disminuir la cantidad de resultados que se mostraran como parte de la búsqueda generalizada y de esta forma considerar estudios recientes.
4. Con base a los criterios de exclusión definidos, se considera la documentación útil y necesaria para realizar el estudio.
5. Se seleccionan los documentos más relevantes y se vuelve aplicar todo el proceso de búsqueda hasta haber aplicado todas las cadenas de búsqueda que se habían definido.

A continuación, en la figura 5 se presenta el de forma gráfica el procedimiento para la selección de los estudios, el cual es generado a partir de los puntos mencionados anteriormente.

Figura 5: Procedimiento para la selección de los estudios. Fuente: Elaboración propia.

1.9.2 Ejecución de la revisión

A continuación, se presenta el proceso aplicado para la selección de fuentes.

1.9.2.1 Ejecución de la selección en la fuente Heliyon

1.9.2.1.1 Selección de estudios iniciales

A continuación, se aplica la búsqueda de estudios iniciales, del cual se muestra su aplicación en la figura 6:

Parámetros de búsqueda aplicados:

- Cyber Kill Chain.
- Advanced Persistent Threats.

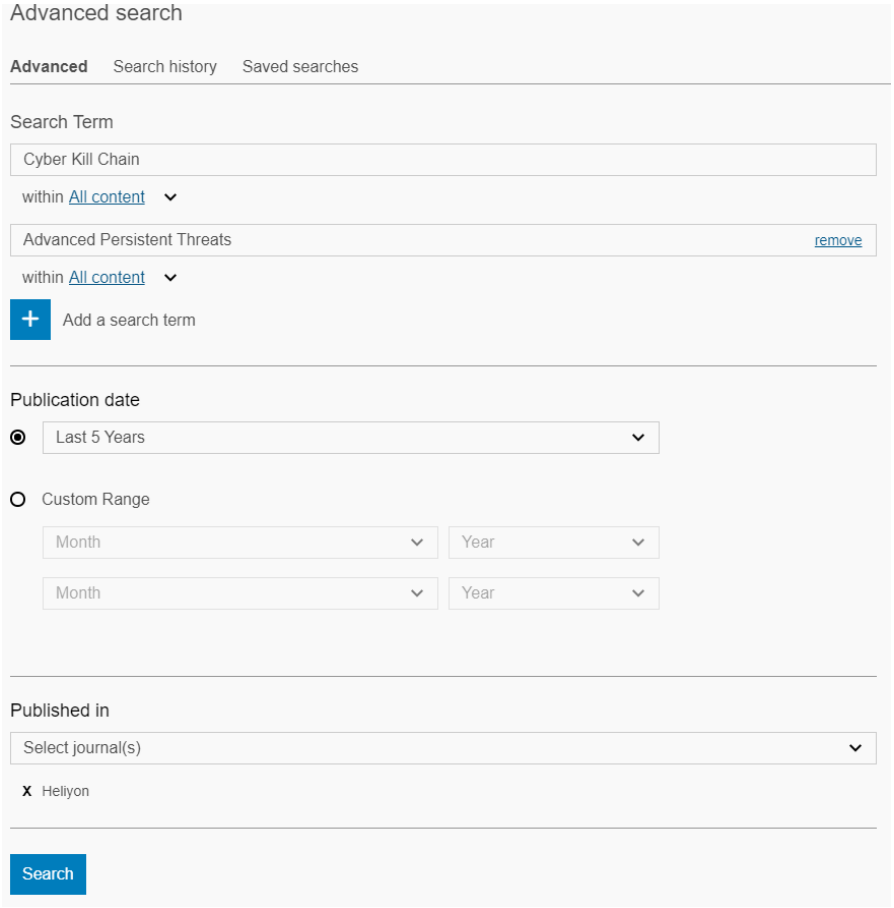


Figura 6: Ejecución de la selección. Fuente Heliyon.

Luego de haber ejecutado la búsqueda con los parámetros específicos y con los filtros aplicados, se obtuvo un resultado que a la vez se identificó como relevante considerándose los criterios de exclusión definidos. A continuación, en la tabla 4 se muestra el detalle de los estudios encontrados.

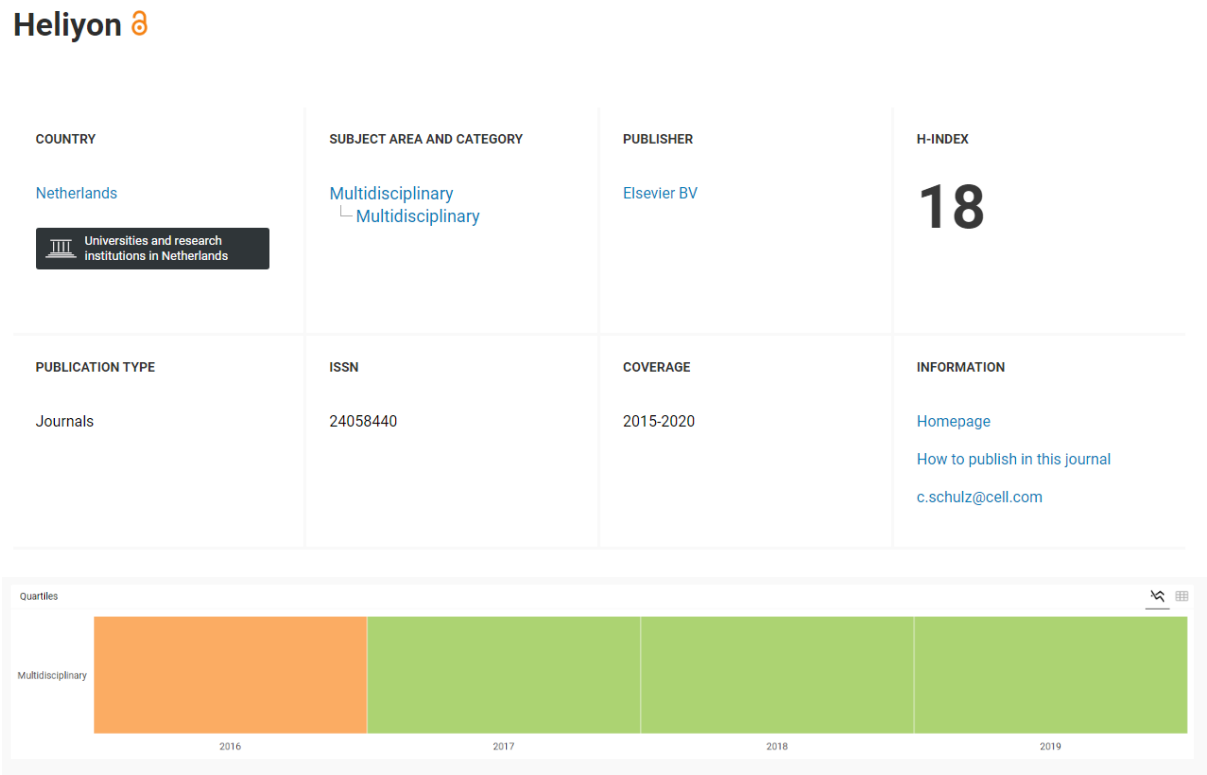
Tabla 4: *Estudios encontrados en Heliyon*

Número	Título	Autores	Año	Dirección URL
1	A review of threat modelling approaches for APT-style attacks	Matt Tatam, Bharanidharan Shanmugam *, Sami Azam, Krishnan Kannoorpatti	2021	https://www.cell.com/heliyon/pdf/S2405-8440(21)00074-8.pdf

Fuente: Elaboración propia.

1.9.2.1.2 Evaluación de la calidad de los estudios

En la figura 7 se demuestra la calidad del artículo seleccionado considerándose la revisión de calidad aplicada a Heliyon.



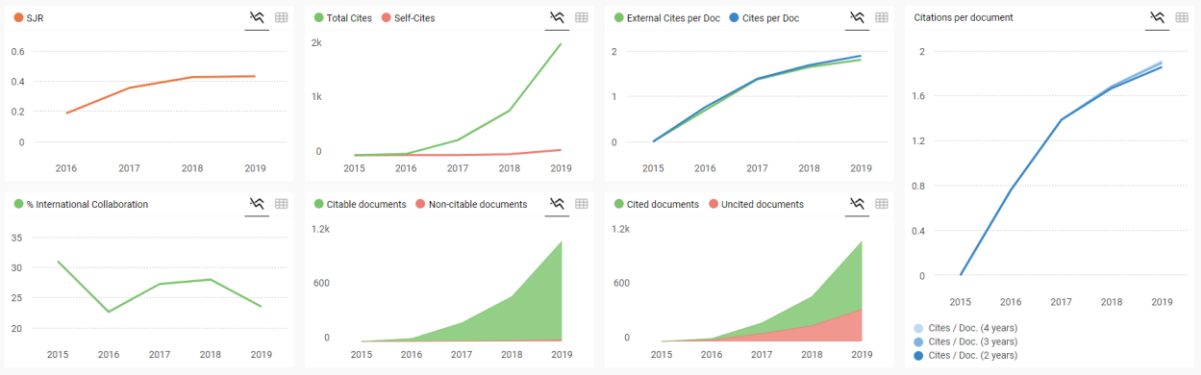


Figura 7: Heliyon validación de calidad de fuentes. Fuente Scimagojr.

1.9.2.1.3 Revisión de la selección

Para definir la selección de estudios primarios se analizan diferentes elementos en el documento, tales como el Abstract y el contenido que conforma cada artículo.

1.9.2.1.4 Extracción de la información

Para extraer la información que se identificara como importante para los estudios primarios, se considera lo siguiente:

- Cyber Kill Chain aplicado a la resolución de problemas relacionados a Advanced Persistent Threats.
- Modelado y análisis sobre Advanced Persistent Threats.
- Consideración de la aplicación de inteligencia y metodologías de mitigación sobre Advanced Persistent Threats.
- Estudios y publicaciones relacionadas a Cyber Kill Chain y Advanced Persistent Threats.

Considerando los puntos anteriores, se muestra en la tabla 5 la información referente a la extracción de la primera fuente.

Tabla 5: *Extracción fuente 1*

Publicaciones de Heliyon	
Título	A review of threat modelling approaches for APT-style attacks
Publicación	Heliyon Volume 7, Issue 1, 2021
Autores	Matt Tatam, Bharanidharan Shanmugam, Sami Azam, Krishnan Kannoorpatti
Referencia	(Tatam, M., Shanmugam, B., Azam, S., & Kannoorpatti, K, 2021). A review of threat modelling approaches for APT-style attacks. Heliyon, Volume 7, Issue 1, e05969
Área	Advanced Persistent Threats, Modelado de amenazas.
Resumen	La aplicación de una estrategia de defensa contra ataques y amenazas requiere de la aplicación de diferentes métodos y mecanismos que permitan su mitigación por lo que se requiere el uso de metodologías en las cuales se aplique un proceso de análisis basado en inteligencia de amenazas para realizar un modelado de amenazas que permita dar trazabilidad de tal manera que logre la identificación y la comprensión sobre posibles amenazas existentes. El presente estudio trata sobre de determinar las limitaciones del modelado de amenazas, las fortalezas y las brechas que se identifiquen. Además, se identifican las posibles mejoras a nivel de

Publicaciones de Heliyon	
	rendimiento y eficiencia para Advanced Persitent Threats.
Aspectos por destacar	DOI: 10.1016/j.heliyon.2021.e05969 El estudio se considera diferentes modelos y metodologías para conocer que brinda cada uno para el tratamiento de amenazas.

Fuente: Elaboración propia.

1.9.2.2 Ejecución de la selección en la fuente Computers and Security

1.9.2.2.1 Selección de estudios iniciales

A continuación, se aplica la búsqueda de estudios iniciales:

Parámetros de búsqueda aplicados:

- Threat.
- Intelligence.
- Attacks.
- Counterattack.

En la figura 8 la ejecución de la selección de los estudios con base a los puntos anteriormente definidos.

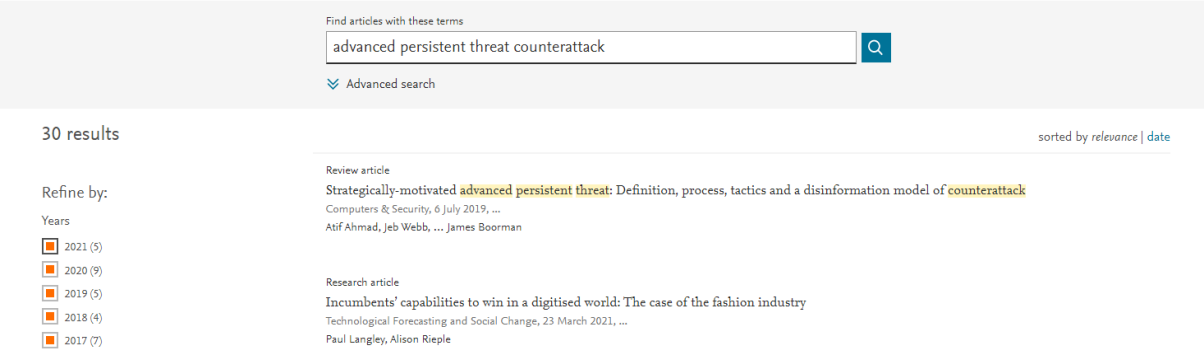


Figura 8: Ejecución de la selección Computers and Security. Fuente: Science Direct.

Luego de haber ejecutado la búsqueda con los parámetros específicos y con los filtros aplicados, se obtuvo 5154 y 30 resultados, de los cuales se seleccionó un documento por cada búsqueda realizada, los cuales se identificaron como relevantes considerándose los criterios de exclusión definidos. A continuación, se muestra en la tabla 6 los estudios encontrados.

Tabla 6: *Estudios encontrados en Computers and Security*

Número	Título	Autores	Año	Dirección URL
2	A survey on technical threat intelligence in the age of sophisticated cyber attacks	Wiem Tounsi, Helmi Rais	2017	https://www.researchgate.net/profile/Wiem-Tounsi/publication/320027747_A_survey_on_technical_threat_intelligence_in_the_age_of_sophisticated_cyber_attacks/links/59fc7cb70f7e9b9968bd9e02/A-survey-on-technical-threat-intelligence-in-the-age-of-sophisticated-cyber-attacks.pdf
3	Strategically-Motivated Advanced Persistent Threat:	Atif Ahmad, Jeb Webb, Kevin C.Desouza	2019	https://www.researchgate.net/profile/Atif-Ahmad-5/publication/334274476_Strategically-Motivated_Advanced_Persistent

Número	Título	Autores	Año	Dirección URL
	Definition, Process, Tactics and a Disinformation Model of Counterattack	, James Boorman		_Threat_Definition_Process_Tactics_and_a_Disinformation_Model_of_Counterattack/links/5d2e395692851cf4408a70fa/Strategically-Motivated-Advanced-Persistent-Threat-Definition-Process-Tactics-and-a-Disinformation-Model-of-Counterattack.pdf

Fuente: Elaboración propia.

1.9.2.2.2 Evaluación de la calidad de los estudios

En la figura 9 se demuestra la calidad del artículo seleccionado considerándose la revisión de calidad aplicada a Computers and Security.

Computers and Security

COUNTRY	SUBJECT AREA AND CATEGORY	PUBLISHER	H-INDEX
United Kingdom Universities and research institutions in United Kingdom	Computer Science Computer Science (miscellaneous) Social Sciences Law	Elsevier Ltd.	86
PUBLICATION TYPE	**ISSN**	**COVERAGE**	**INFORMATION**
Journals	01674048	1982-2020	Homepage How to publish in this journal

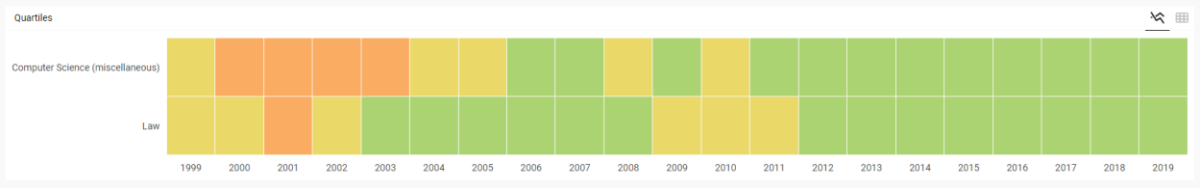


Figura 9: Computers and Security validación de calidad de fuentes. Fuente: Scimagojr.

1.9.2.2.3 Revisión de la selección

Para definir la selección de estudios primarios se analizan diferentes elementos en el documento, tales como el Abstract y el contenido que conforma cada artículo.

1.9.2.2.4 Extracción de la información

Para extraer la información que se identificara como importante para los estudios primarios, se considera lo siguiente:

- Cyber Kill Chain aplicado a la resolución de problemas relacionados a Advanced Persistent Threats.
- Modelado y análisis sobre Advanced Persistent Threats.
- Consideración de la aplicación de inteligencia y metodologías de mitigación sobre Advanced Persistent Threats.
- Estudios y publicaciones relacionadas a Cyber Kill Chain y Advanced Persistent Threats.

Considerando los puntos anteriores, se muestra en la tabla 7 la información referente a la extracción de la segunda fuente.

Tabla 7: *Extracción fuente 2*

Publicaciones de Computers and Security	
Título	A survey on technical threat intelligence in the age of sophisticated cyber attacks
Publicación	Computers & security, 72, 212-233.
Autores	Wiem Tounsi, Helmi Rais

Publicaciones de Computers and Security	
Referencia	Wiem Tounsi, Helmi Rais, “A survey on technical threat intelligence in the age of sophisticated cyber attacks”, 2018 Computers & Security, Volume 72, pp. 212-233. ISSN 0167-4048. doi: 10.1016/j.cose.2017.09.001.
Área	Ciber ataques. Detección de amenazas. Inteligencia de amenazas. Gestión de riesgos. Technical Threat Indicators (TTI). Análisis de Big Data.
Resumen	Las ciber amenazas actuales son más avanzadas por lo cual requieren de la aplicación de diferentes estrategias y mecanismos de seguridad con el fin de lograr establecer una metodología que coadyuve a su mitigación. Estas amenazas tienen capacidad de evadir, resistir realizar procesos complejos por lo cual se requiere de la aplicación de inteligencia de amenazas con el fin de obtener y estudiar toda la información relacionada a estas amenazas con el fin de prevenir ataques cibernéticos o bien aplicar un proceso de recuperación ante desastres producidos por estas amenazas. Para la inteligencia de amenazas se requiere recolectar la mayor cantidad de información posible que sirva como evidencia además para conocer lo más que se pueda sobre las amenazas por lo cual

Publicaciones de Computers and Security	
	también se utilizan los Technical Threat Indicators con el fin de generar dicha información en tiempo real y que esta sea compartida entre organizaciones y esté disponible para la aplicación de diferentes estrategias según convenga. Por lo cual se analizan diferentes herramientas existentes sobre los indicadores de amenazas técnica por lo que se hace una comparación y se generan sugerencias sobre cómo se puede mejorar la compartición de información sobre amenazas.
Aspectos por destacar	El estudio hace un análisis profundo sobre los Technical Threat Indicators y brinda realimentación sobre cómo se puede aplicar y mejorar para el tratamiento de amenazas avanzadas.

Fuente: Elaboración propia.

Considerando el mismo objetivo de búsqueda, se muestra en la tabla 8 la información referente a la extracción de la tercera fuente.

Tabla 8: *Extracción fuente 3*

Publicaciones de Computers and Security	
Título	Strategically-Motivated Advanced Persistent Threat: Definition, Process, Tactics and a Disinformation Model of Counterattack
Publicación	Computers & Security, 86, 402-418.
Autores	Atif Ahmad; Jeb Webb; Kevin C.Desouza; James Boorman

Publicaciones de Computers and Security	
Referencia	A. Ahmad; J. Webb; K. C. Desouza; J. Boorman, “Strategically-motivated advanced persistent threat: Definition, process, tactics and a disinformation model of counterattack,” Computers & Security, Volume 86, pp. 402-418. ISSN 0167-4048. doi: 10.1016/j.cose.2019.07.001.
Área	Advanced Persistent Threats. Information Security Management. Strategic Disinformation. Tactics, Techniques, and Procedures (TTPs).
Resumen	En este estudio se propone realizar un análisis sobre las amenazas persistentes avanzadas con el fin de desarrollar un modelo sobre las etapas de ejecución de una operación de una amenaza persistente avanzada con el fin de hacer un análisis sobre las amenazas persistentes avanzadas estratégicamente motivadas (S-APT) y de esta forma generar un modelo que sirva para explicar cómo la desinformación puede ser utilizada para Finalmente, presentamos un modelo de desinformación general, derivado de la teoría de la conciencia de situación, y explicar cómo se puede utilizar la desinformación para atacar la conciencia situacional y la toma de decisiones tanto por parte de los operadores S-APT como de quienes los respaldan.

Publicaciones de Computers and Security	
Aspectos por destacar	Análisis y definición de modelos para amenazas persistentes avanzadas y sus variantes considerándose la teoría de la conciencia situacional.

Fuente: Elaboración propia.

1.9.2.3 Ejecución de la selección en la fuente IEEE

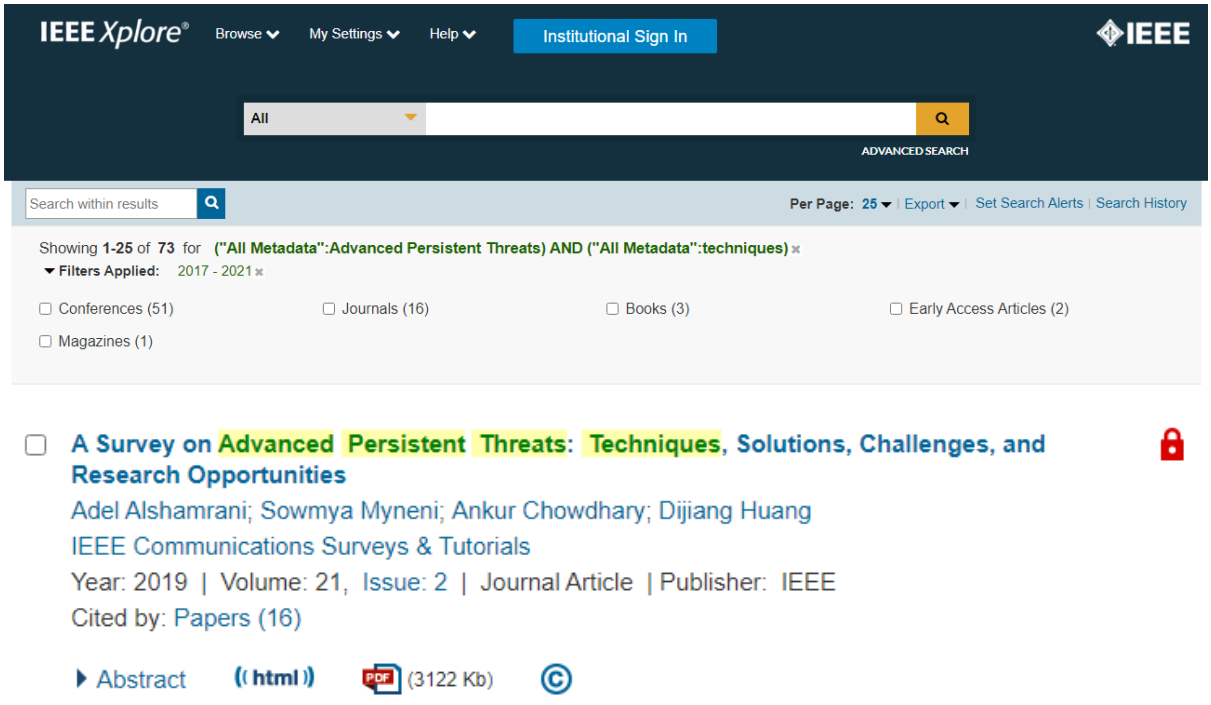
1.9.2.3.1 Selección de estudios iniciales

A continuación, se aplica la búsqueda de estudios iniciales:

Parámetros de búsqueda aplicados:

- Advanced Persistent Threats.
- Techniques.

En la figura 10 la ejecución de la selección de los estudios con base a los puntos anteriormente definidos.



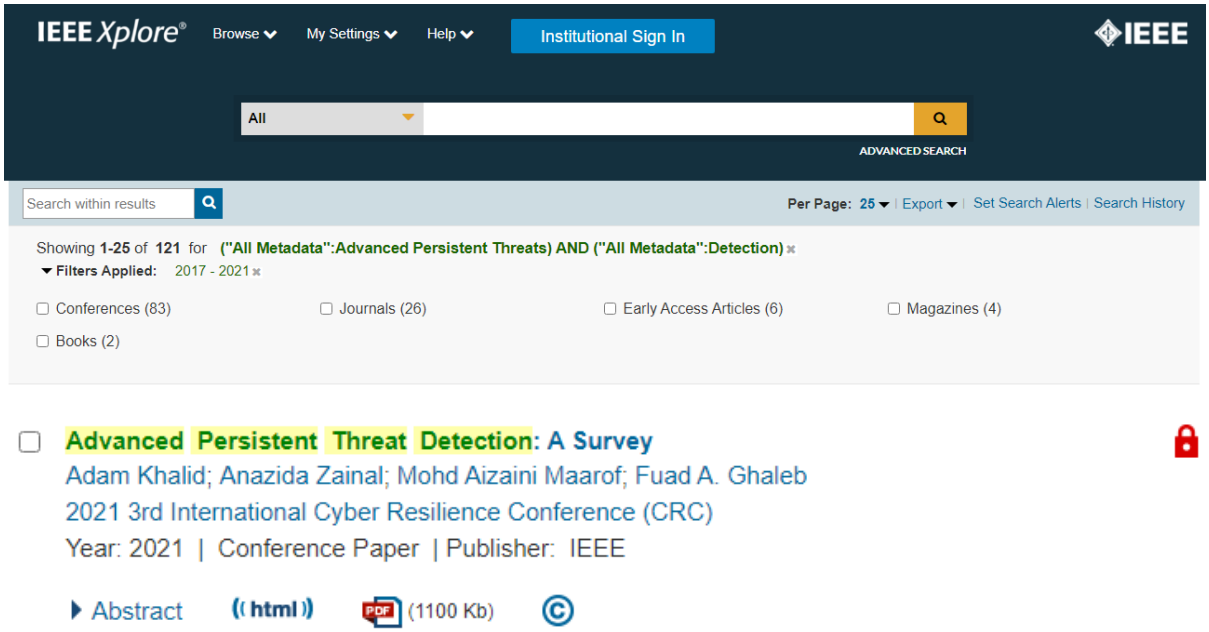


Figura 10: Ejecución de la selección IEEE. Fuente: IEEE Xplore.

Luego de haber ejecutado la búsqueda con los parámetros específicos y con los filtros aplicados, se obtuvo 73 y 121 resultados, de los cuales se seleccionó un documento por cada búsqueda realizada, los cuales se identificaron como relevantes considerándose los criterios de exclusión definidos. A continuación, en la tabla 9 se muestra el detalle de los estudios encontrados.

Tabla 9: *Estudios encontrados en IEEE*

Número	Título	Autores	Año	Dirección URL
4	A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges, and Research Opportunities	Adel Alshamrani, Sowmya Myneni, Ankur Chowdhary, Dijiang Huang	2019	https://ieeexplore.ieee.org/document/8606252

Número	Título	Autores	Año	Dirección URL
5	Advanced Persistent Threat Detection: A Survey	Adam Khalid, Anazida Zainal, Mohd Aizaini Maarof, Fuad A. Ghaleb	2021	https://ieeexplore.ieee.org/document/9392626

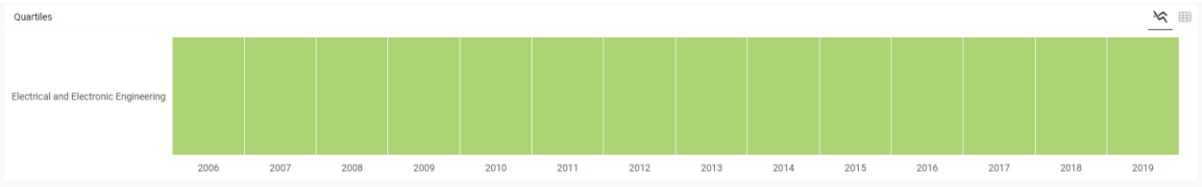
Fuente: Elaboración propia.

1.9.2.3.2 Evaluación de la calidad de los estudios

En la figura 11 se demuestra la calidad del artículo seleccionado considerándose la revisión de calidad aplicada a IEEE.

IEEE Communications Surveys and Tutorials

COUNTRY	SUBJECT AREA AND CATEGORY	PUBLISHER	H-INDEX
United States Universities and research institutions in United States	Engineering Electrical and Electronic Engineering	Institute of Electrical and Electronics Engineers Inc.	169
PUBLICATION TYPE	**ISSN**	**COVERAGE**	**INFORMATION**
Journals	1553877X	2005-2020	Homepage How to publish in this journal ydlin@cs.nctu.edu.tw



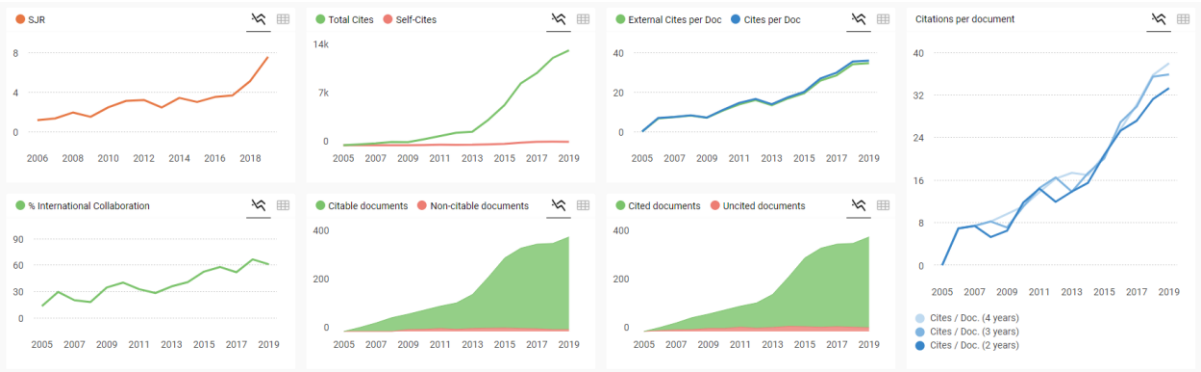


Figura 11: IEEE validación de calidad de fuentes. Fuente: Scimagojr.

1.9.2.3.3 Revisión de la selección

Para definir la selección de estudios primarios se analizan diferentes elementos en el documento, tales como el Abstract y el contenido que conforma cada artículo.

1.9.2.3.4 Extracción de la información

Para extraer la información que se identificara como importante para los estudios primarios, se considera lo siguiente:

- Cyber Kill Chain aplicado a la resolución de problemas relacionados a Advanced Persistent Threats.
- Modelado y análisis sobre Advanced Persistent Threats.
- Consideración de la aplicación de inteligencia y metodologías de mitigación sobre Advanced Persistent Threats.
- Estudios y publicaciones relacionadas a Cyber Kill Chain y Advanced Persistent Threats.

Considerando los puntos anteriores, se muestra en la tabla 10 la información referente a la extracción de la cuarta fuente.

Tabla 10: *Extracción fuente 4*

Publicaciones de IEEE	
Título	A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges, and Research Opportunities
Publicación	IEEE Communications Surveys & Tutorials
Autores	Adel Alshamrani, Sowmya Myneni, Ankur Chowdhary, Dijiang Huang
Referencia	A. Alshamrani, S. Myneni, A. Chowdhary and D. Huang, "A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges, and Research Opportunities," IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1851-1877, Secondquarter 2019. doi: 10.1109/COMST.2019.2891891.
Área	amenazas persistentes avanzadas. Detección de intrusiones.
Resumen	Las amenazas persistentes avanzadas o APTs han sido objeto de uso por parte de empresas privadas como por parte de naciones o países las cuales a su vez buscan mecanismos de protección sobre las mismas dado que pueden ser aprovechadas por su contra parte. Estos ataques siempre han sido caracterizados por su alto nivel de sofisticación y han tenido mayor relevancia en el sector empresarial. A medida que avanzan las amenazas persistentes avanzadas, cada vez las herramientas y mecanismos de protección convencionales van siendo

Publicaciones de IEEE	
	menos efectivos contra este tipo de ataques por lo cual es necesario implementar soluciones basadas en la correlación y en el análisis de comportamiento tanto de los usuarios como de los sistemas. Por lo cual se busca el reconocimiento de métodos y técnicas las cuales se pueden aplicar en cualquiera de las etapas de un ataque APT, así como de un estudio detallado sobre métodos de monitoreo y de mitigación que sean aplicables para los sistemas en la red.
Aspectos por destacar	El estudio hace un análisis profundo sobre las amenazas persistentes avanzadas de tal manera que se da una explicación completa que sirva de base para la definición de conceptos, así como para comprender con mayor detalle el funcionamiento de este tipo de amenazas. También se muestra que otros estudios o investigaciones se pueden aplicar para continuar desarrollando el conocimiento sobre este tipo amenazas.

Fuente: Elaboración propia.

Considerando el mismo objetivo de búsqueda, se muestra en la tabla 11 la información referente a la extracción de la tercera fuente.

Tabla 11: *Extracción fuente 5*

Publicaciones de IEEE	
Título	Advanced Persistent Threat Detection: A Survey
Publicación	2021 3rd International Cyber Resilience Conference (CRC)
Autores	Adam Khalid; Anazida Zainal; Mohd Aizaini Maarof; Fuad A. Ghaleb
Referencia	A. Khalid, A. Zainal, M. A. Maarof and F. A. Ghaleb, "Advanced Persistent Threat Detection: A Survey," 2021 3rd International Cyber Resilience Conference (CRC), 2021, pp. 1-6. doi: 10.1109/CRC50527.2021.9392626.
Área	Amenazas persistentes avanzadas. Aprendizaje automático. Detección de intrusiones.
Resumen	Se han definido diferentes tipos de enfoques para la detección de las amenazas persistentes avanzadas dado que los ataques basados en este tipo de amenazas tienen objetivos muy específicos los cuales muchos son realizados por organizaciones muy bien financiadas y normalmente son campañas a largo plazo. Además, se ha definido que las APT siguen un proceso de Kill Chain sobre el cual se pueden identificar métodos de detección e intrusión.
Aspectos por destacar	Muestra la forma en la que operan las amenazas persistentes avanzadas.

Publicaciones de IEEE	
	Identifica y muestra cómo se utilizan los diferentes métodos de detección e intrusión. Fundamenta la relación entre las amenazas persistentes avanzadas y el proceso de Kill Chain.

Fuente: Elaboración propia.

1.9.3 Resumen de los resultados

En la tabla 12, se muestran la cantidad de estudios que se obtuvieron al aplicar la búsqueda sobre cada una de las fuentes definidas de las cuales se analizaron un total de 5379 estudios para considerar cinco como parte de la investigación inicial.

Tabla 12: *Análisis de resultados*

Fuente	Estudios	Considerados
Heliyon	1	1
Computers & Security	5154 y 30	2
IEEE	73 y 121	2
Total	5379	5

Fuente: Elaboración propia.

Capítulo 2. Marco Conceptual

Actualmente, muchas organizaciones son afectadas por ataques de Día Cero o amenazas persistentes avanzadas a nivel mundial por lo que su estudio y análisis se han vuelto altamente importantes para afrontar las principales amenazas generadas por este tipo de ataques. A la vez, este tipo de ataques cada vez se van volviendo más complejos conforme avanza la tecnología, dado que también se aprovechan muchas herramientas avanzadas, las cuales son creadas a partir de los más recientes avances, además que el desarrollo de este tipo de ataques normalmente es ejecutado por grupos de hackers altamente sofisticados y bien financiados, tanto por empresas como por gobiernos para llevar a cabo ataques específicos y a gran escala, por lo que a su vez su identificación -para efectos de defensa- es complejo. Normalmente, este tipo de ataques son difíciles de identificar y de rastrear, por lo que a su vez es difícil de identificar a los responsables.

Además, se han desarrollado diferentes mecanismos de protección, así como modelos de seguridad para la protección de la información, para dar respuesta a este tipo de ataques, así como también existen datos e información de los grupos que mayormente tienen participación en este tipo de ataques, donde incluso, empresas y diferentes tipos de organizaciones trabajan en conjunto para retroalimentar esta información en tiempo real y de esta manera lograr un conocimiento más aproximado sobre los ataques que se ejecutarán, o bien para identificar los grupos encargados de ejecutarlos.

También se han desarrollado modelos de seguridad, para aplicar diferentes mecanismos de protección que respondan a este tipo ataques, así como para ayudar a las organizaciones a establecer estrategias de defensa.

Se generó la nube de conceptos a partir de diferentes palabras con el fin de extraer aquellos más importantes, que normalmente tienden a identificarse en la mayoría de los artículos incluidos en el estado de la cuestión. En la figura 12 se muestra de forma gráfica algunas de las palabras generadas.

Figura 12: Nube de palabras. Fuente: Elaboración propia. Elaborado usando el sitio https://www.nubedepalabras.es/

A continuación, se presentan los conceptos más utilizados y que se consideran como de mayor importancia para la investigación.

2.1 Conceptos sobre amenazas persistentes avanzadas

Como parte de fundamentar los distintos conceptos relacionados, tanto a las amenazas persistentes avanzadas como a Cyber Kill Chain, se procede a establecer los conceptos relacionados.

Cabe mencionar que el alcance de este trabajo comprende en su mayoría la comprensión sobre amenazas persistentes avanzadas, por lo que la conceptualización de este trabajo se centra sobre este concepto.

- Tipos de ataques:
    - Zero Day.
    - Botnets.
    - DDoS.

    - Malware.
    - Phishing.
    - Rasomware.
- Metodologías:
    - Cyber Kill Chain.
    - MITRE ATT&CK.
- Métodos de detección:
    - Detección de anomalías.
    - Coincidencia de patrones.
- Métodos de mitigación:
    - Reactivos.
    - Proactivos.
- Análisis de inteligencia:
    - Tactics, Techniques, and Procedures (TTP):
        - Tactical Threat Intelligence.
        - Technical Threat Intelligence.
        - Strategic Threat Intelligence.
        - Operational Threat Intelligence.
    - Indicadores de análisis:
        - Indicators of compromise (IOC).
        - Indicators of Attack (IoA).
        - Indicators of Exposure (IoE).
    - Intercambio de información:
        - CSIRT-CR

- Computer Emergency Response Teams (CERT).
- The Forum for Incident Response and Security Teams (FIRST).
- The Euro-CERT group (TF-CSIRT).
- The European Government CSIRTs group (EGC).
- ENISA.
- NIST.
- MITRE.
- No More Ransom.
- Information Sharing and Analysis Centers (ISAC).

A continuación, se muestra en la figura 13 el mapa conceptual del objeto de estudio generado a partir de los puntos anteriormente definidos.

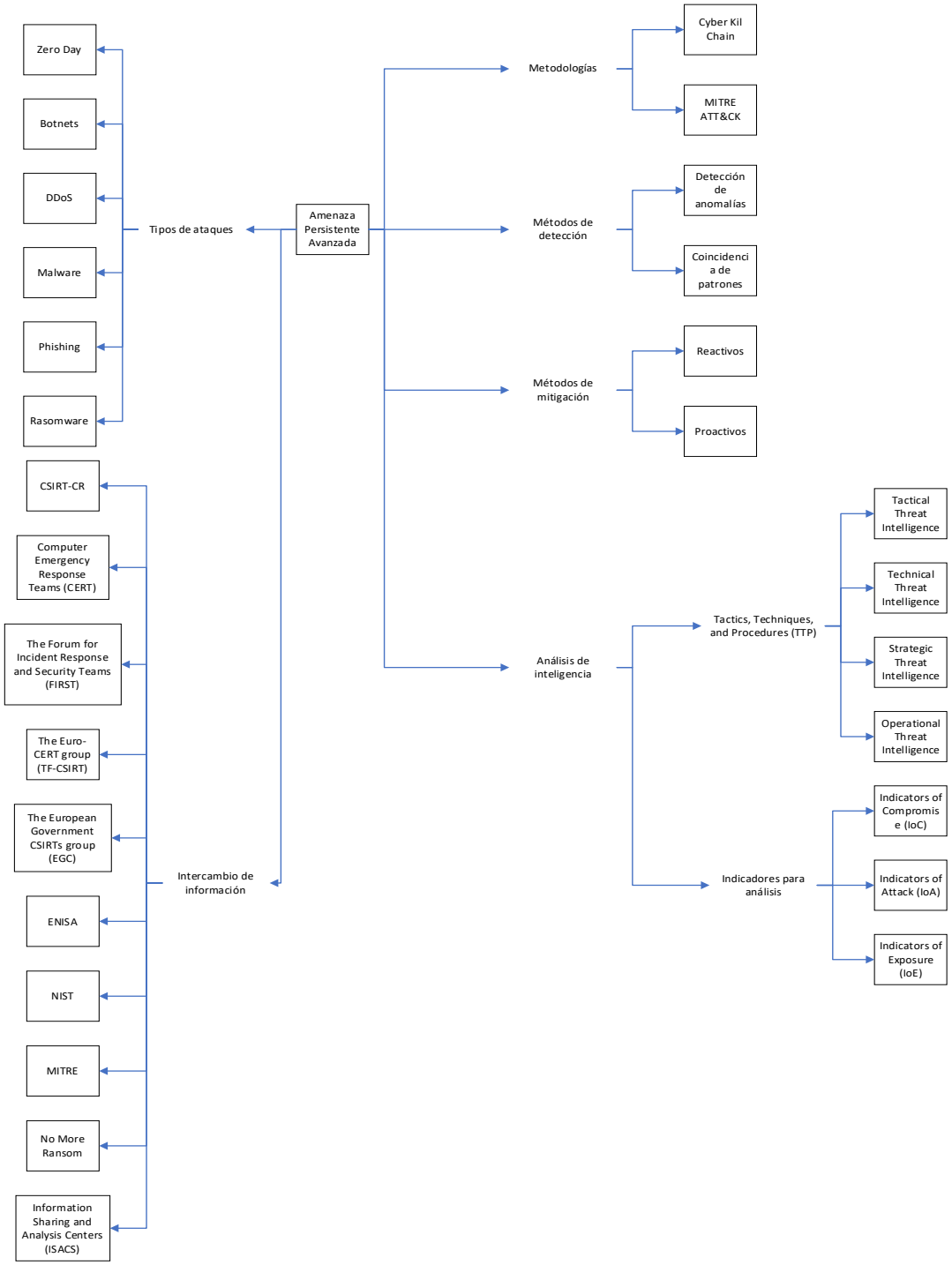


Figura 13: Mapa conceptual del objeto de estudio. Fuente: Elaboración propia.

2.1.1 Definición de amenaza persistente avanzada (APT)

Según (Quintero-Bonilla, S., & Martín del Rey, A. 2020) una amenaza persistente avanzada (APT) se define como un ciberataque dirigido y muy sofisticado. Por lo cual estos son desarrollados de manera muy específica dependiendo del

objetivo del ataque. Al decirse que son específicos se refiere a que, a diferencia de otros tipos de ataques más comunes, estos son desarrollados considerando las vulnerabilidades existentes en una infraestructura de sistemas de información, por lo cual se desarrollan de forma muy específica de tal manera que solo afecten a los sistemas que forman parte de dicha infraestructura.

Por esta razón los mismos autores indican que los administradores de TI necesitan herramientas que permitan la detección temprana de estos ataques para proteger los sistemas de información de las organizaciones a las que pertenecen.

Además, Bahrami, P. N., Dehghantanha, A., Dargahi, T., Parizi, R. M., Choo, K. K. R., & Javadi, H. H. (2019) definen que los ciberataques son cada vez más sofisticados, especialmente a medida que los países tecnológicamente avanzados empiezan a brindar más énfasis en adquirir y fortalecer sus capacidades ciber ofensivas y defensivas.

Por lo cual se conoce el alto nivel de sofisticación de estos ataques y que cada vez más países están haciendo esfuerzos en conjunto para tratar de mitigar este tipo de ataques. Esta preocupación existe dado que muchas organizaciones, así como gobiernos de todo el mundo dependen cada vez más del uso de los datos y de la información administrada a través de sistemas para sus operaciones diarias. Esto claramente genera una brecha de seguridad muy importante de atender por parte de equipos de TI, de tal manera que sea necesario la implementación de estrategias que permitan administrar estos riesgos.

Según Bahrami, P. N., Dehghantanha, A., Dargahi, T., Parizi, R. M., Choo, K. K. R., & Javadi, H. H. (2019), la sofisticación de los ataques se debe en parte a la dependencia cada vez mayor de las organizaciones gubernamentales y comerciales de los centros de datos y las redes de computadoras y la importancia de obtener acceso a dicha información y sistemas para asegurar ventajas estratégicas y políticas. Por ejemplo, se ha observado que ha habido un aumento en el número de amenazas persistentes avanzadas (APT) dirigidas tanto a organizaciones gubernamentales como comerciales.

2.1.2 Definición de grupos APT

Los grupos APT se encargan de ejecutar las amenazas persistentes avanzadas, los cuales tienen un alto conocimiento en diferentes ramas de la informática y normalmente son contratados por empresas o gobiernos con capacidad de financiamiento para llevar a cabo este tipo operaciones. Normalmente emplean herramientas desarrolladas a la medida por estos mismos grupos, o bien parte del código fuente u otra herramienta que pueda funcionar de soporte se puede obtener de fuentes.

Según Tatam, M., Shanmugam, B., Azam, S., & Kannoorpatti, K. (2021) las APT son ataques subrepticios que son empleados por adversarios conocedores e ingeniosos, cuya intención es comprometer la confidencialidad, integridad y disponibilidad de la información y/o infraestructura crítica. El ataque de una APT está bien planificado y consta de múltiples fases, que están diseñadas para alcanzar y persistir en el sistema objetivo sin detección. Los APT eligen sus herramientas en función del entorno y los pasos necesarios para lograr su objetivo. La capacidad de las APT ha evolucionado con el tiempo a medida que estos grupos continúan expandiendo sus objetivos actuales y, por lo tanto, implementando Tácticas, Técnicas y Procedimientos, TTP por sus siglas en inglés, mejoradas o nuevas. Estos grupos pueden desarrollar malware apropiados para su propósito y métodos de exfiltración de datos.

Tatam, M., Shanmugam, B., Azam, S., & Kannoorpatti, K. (2021), mencionan que el desarrollo de los marcos de trabajo como Cyber Kill Chain y MITRE ATT&CK se han desarrollado a partir de años de observaciones APT e inteligencia de amenazas relacionada. Por lo cual, estos marcos de trabajo normalmente son los más apropiados de aplicar en caso de tratar con grupos APT, así como sus ataques.

2.1.3 Definición de ataque de día cero.

El ataque de día cero aprovecha vulnerabilidades en software o sistemas, los cuales son vulnerables y a los cuales no se les ha desarrollado o aplicado una solución para atender dichas vulnerabilidades como parches o actualizaciones, además de que no son difícilmente de detectar por los sistemas de seguridad dependiendo de su capacidad.

Según Bahrami, P. N., Dehghantanha, A., Dargahi, T., Parizi, R. M., Choo, K. K. R., & Javadi, H. H. (2019), la explotación de día cero tiene como objetivo utilizar una falla de software que se desconoce y que no tiene parches ni correcciones. Los exploits de día cero no son detectables con el mecanismo de protección de seguridad tradicional.

Normalmente los ataques de día cero se suelen asociar a amenazas persistentes avanzadas, dado que estos ataques son desarrollados por atacantes APT, independiente de que pertenezcan a un grupo APT o no, dado su alto nivel de complejidad de desarrollo lo que conlleva a que el o los atacantes deban de tener un elevado conocimiento informático.

Bahrami, P. N., Dehghantanha, A., Dargahi, T., Parizi, R. M., Choo, K. K. R., & Javadi, H. H. (2019), mencionan que solo los atacantes avanzados son capaces de encontrar vulnerabilidades de día cero y escribir exploits de día cero. Además, mencionan como ejemplo que el grupo Axiom lanzó una serie de ataques en el Proyecto Elderwood en 2009 contra objetivos de alto perfil en América del Norte y utilizó gran cantidad de vulnerabilidades de día cero para entregar un malware. El número de exploits de día cero utilizados por un atacante APT revela su alto nivel de competencia técnica. Los actores de APT son muy cuidadosos al usar exploits de día cero, ya que cualquier detección de riesgo de uso podría llevar a perder un arma valiosa contra otros objetivos.

2.1.4 Definición de Cyber Kill Chain.

El concepto de Cyber Kill Chain llamado en inglés CKC por sus siglas en inglés, es un marco de trabajo de seguridad propuesto por la empresa estadounidense Lockheed Martin Corporation encargada del desarrollo de tecnología aeroespacial, de armas, defensa, seguridad y tecnologías avanzadas. Como mencionan Quintero-Bonilla, S., & Martín del Rey, A. (2020), este marco de trabajo busca comprender cómo funciona un ataque para enriquecer la comprensión de las tácticas, técnicas y procedimientos utilizados por los atacantes.

Este marco de trabajo está compuesto por siete etapas descritas por Quintero-Bonilla, S., & Martín del Rey, A. (2020) de la siguiente forma:

1. Reconocimiento: el atacante realiza un reconocimiento preliminar de la red de la organización, utilizando técnicas de spear phishing, escaneo de puertos e ingeniería social.
2. Armamento: el atacante crea una carga útil que se envía a la víctima. Por lo general, consiste en un exploit con una entrega RAT / troyan.
3. Entrega: La carga útil creada se envía a la víctima a través de correo, sitios web o dispositivos de eliminación.
4. Explotación: el atacante ejecuta la explotación que se le ha enviado a la víctima.
5. Instalación: un troyano y/o un troyano de acceso remoto (RAT) se instala cuando el atacante obtiene acceso al sistema.
6. Comando y control: el software de acceso remoto se conecta a C&C del atacante.
7. Acciones y objetivos: El atacante realiza la exfiltración de datos comprometiendo la integridad y disponibilidad de los datos. Esta etapa puede durar semanas, meses o incluso años.

Es claro que la modalidad de operación de los ataques pueden variar, por lo que a pesar de que se conoce un patrón de comportamiento, el marco de trabajo de Cyber Kill Chain es muy dinámico en el sentido en que puede ser aplicado para la mayoría de los ataques conocidos; sin embargo, uno de sus mayores aportes se relaciona con las amenazas persistentes avanzadas, ya que muy pocos marcos de trabajo de seguridad fueron preparados o están desarrollados para atender este tipo de amenazas, donde el principal es el ataque de Día Cero, pues la víctima y las empresas de ciber seguridad desconocen completamente el ataque, tanto su día de ejecución como sus patrones de comportamiento como para generar una respuesta que mitigue dicho ataque.

2.1.5 Definición de amenazas de nueva generación

Las amenazas de nueva generación tienen la capacidad de propagarse fácilmente a través de cualquier medio sin importar la arquitectura, los equipos o, incluso, los sistemas de seguridad implementados de tal manera que tienen la

capacidad de adaptarse a cualquier ambiente de TI y por lo tanto también son sofisticados. De igual manera, este concepto se suele asociar a los ataques APT por lo que tienen una fuerte de relación con Cyber Kill Chain como marco de trabajo a aplicar sobre este tipo de amenazas.

Según Tounsi, Wiem & Rais, Helmi. (2017), las amenazas de nueva generación son de múltiples vectores y, a menudo, de múltiples etapas: de múltiples vectores, porque los ataques pueden usar múltiples medios de propagación (por ejemplo, web, correo electrónico, aplicaciones) y de múltiples etapas, ya que los ataques pueden infiltrarse en las redes, propagarse y, en última instancia, exfiltrar los datos valiosos. Estas amenazas de nueva generación que dan lugar a nuevos escenarios de ataque pueden entenderse desde la perspectiva defensiva de una “Kill chain”. Un "Kill chain" es una secuencia de etapas necesarias para que un atacante se infiltre con éxito en una red y extraiga datos de ella.

2.1.6 Definición de amenazas polimórficas

Las amenazas polimórficas son amenazas que tienen la capacidad de evolucionar o cambiar su comportamiento durante la ejecución de un ataque. Generalmente poseen la capacidad de adaptarse a diferentes condiciones o ambientes de tal manera que logren tornarse indetectables, o bien cumplir el objetivo para el cual fueron diseñadas. Precisamente por esta misma característica de cumplir con el objetivo para el cual fueron diseñadas, pueden cambiar, pero mantienen sus características de comportamiento básicas las cuales pueden mostrar patrones.

Según detallan Tounsi, Wiem & Rais, Helmi. (2017) las amenazas polimórficas son ataques cibernéticos, como virus, gusanos o troyanos que cambian constantemente. La evolución de las amenazas polimórficas puede ocurrir de diferentes maneras (por ejemplo, cambios de nombre de archivo y compresión de archivos). A pesar de la apariencia cambiante del código en una amenaza polimórfica, después de cada mutación, la función esencial generalmente sigue siendo la misma. Por ejemplo, un malware destinado a actuar como registrador de teclas seguirá realizando esa función, aunque su firma haya cambiado.

Capítulo 3. Marco Metodológico

3.1 Tipo de Investigación

Debido a que este proyecto tiene como objetivo la evaluación de la metodología de Cyber Kill Chain en la aplicación sobre amenazas persistentes avanzadas y dado que se requiere también de una evaluación por parte del estado en materia de seguridad de la información respecto a estas amenazas, se considera que la investigación corresponde a una investigación evaluativa.

Se requiere de investigar la metodología Cyber Kill Chain sobre amenazas APT y evaluar qué se ha desarrollado y que no se en Costa Rica en materia de seguridad de la información en relación con amenazas APT. En Costa Rica se ha promovido la seguridad de la información y por lo tanto, existen muchas investigaciones relacionadas a la metodología Cyber Kill Chain y las amenazas APT; sin embargo, nunca se ha investigado si en Costa Rica se han considerado a las amenazas APT como parte de su estrategia de seguridad de la información por lo que se busca definir una estrategia de seguridad de la información en Costa Rica que considere a las amenazas APT y como parte de la misma estrategia definir una metodología para el tratamiento de estas amenazas como lo es Cyber Kill Chain.

3.2 Alcance investigativo

Considerando la definición de (Hernández et al, 2015) sobre los estudios de alcance exploratorio, en el cual se específica:

> "… se realizan cuando el objetivo es examinar un tema o problema de investigación poco estudiado, del cual se tienen muchas dudas o no se ha abordado antes. Es decir, cuando la revisión de la literatura reveló que tan sólo hay guías no investigadas e ideas vagamente relacionadas con el problema de estudio, o bien, si deseamos indagar sobre temas y áreas desde nuevas perspectivas".

Si bien es cierto que a nivel de la revisión de literatura existen estudios que muestran de manera muy completa cómo es que funcionan las amenazas APT y la efectividad de la metodología Cyber Kill Chain sobre este tipo de amenazas, esto no se ha analizado desde la perspectiva de aplicación en el ámbito nacional, por tanto

se debe considerar los mismos desde una perspectiva diferente lo cual define una perspectiva innovadora o bien considerando un paradigma diferente, donde se busca adaptar la aplicación de dicha metodología sobre una estrategia de seguridad de la información en el país de tal forma que se logre atender este tipo de amenazas en el país.

3.3 Enfoque

Dado que esta investigación se centra principalmente en estudiar las amenazas persistentes avanzadas con el fin de proponer una estrategia de seguridad de la información que considere a la metodología Cyber Kill Chain como propuesta de solución primaria; se deben analizar diferentes aspectos que se deben considerar para la correcta evaluación de este estudio, como el contraste entre diferentes teorías o conceptos como para establecer un mayor contexto que sirva para explicar con mayor profundidad el porqué es útil la aplicación de la metodología Cyber Kill Chain sobre las amenazas persistentes avanzadas, por lo cual se orienta a la inferencia de resultados y además se establece el uso del método inductivo, por lo cual esta investigación mantiene un enfoque cualitativo, dado que como resultado se espera obtener una estrategia de seguridad de la información que considere los diferentes aspectos estudiados, pero originando nuevas teorías o conocimientos que sirvan para mejorar el estado de la seguridad del país. A la vez se establece mantener un enfoque cuantitativo, dado que se desea conocer distintos aspectos específicos sobre la situación actual de Cyber Kill Chain en el país, por lo que se mantiene un enfoque mixto de la investigación.

3.4 Diseño

El diseño de la investigación es evaluativo, pues se pretende establecer una mejora a nivel de seguridad de la información en el país, donde la innovación radica en la consideración de las amenazas persistentes avanzadas.

Para realizar dicha investigación se establece lo siguiente:

- Estudiar en profundidad el concepto de amenazas persistentes avanzadas y otros conceptos que tengan relación con este. Por lo cual se hace una extensión de estos hasta haber considerado todos aquellos que sirvan de base para la investigación.

- Brindar, como parte del estudio de conceptos, mayor énfasis al de Cyber Kill Chain, pues es el que se está tomando como punto central en la investigación y como parte de la propuesta de solución para esta investigación, por lo tanto, se da un mayor énfasis en desarrollar la investigación considerando principalmente a las amenazas persistentes avanzadas y a la metodología de Cyber Kill Chain.
- Dar continuación a la investigación estudiando qué se ha hecho a nivel país o qué estrategias se han implementado con el fin de que sirva como base un mayor conocimiento sobre este tema.
- Estudiar y analizar qué han hecho otros países respecto a este tema para identificar si existen estrategias que se puedan aprovechar de tal manera que sirvan para esta investigación.
- Establecer la estrategia de seguridad de la información relacionada a las amenazas persistentes avanzadas.
- Realizar una síntesis de todo el trabajo elaborado y establecer las conclusiones.

3.5 Población y muestreo

Para esta investigación no es aplicable el estudio sobre población y muestreo, ya que no se aplica ningún tipo de experimentación que contemple estos dos conceptos.

En una investigación, la muestra representa todo aquel subgrupo el cual es parte de la población de estudio sobre la cual se van a tomar o extraer datos. Según Sampieri et al. (2014: 173) la muestra es un "… subgrupo del universo o población del cual se recolectan los datos y que debe ser representativo de ésta".

En esta investigación, la muestra se centra prácticamente sobre los individuos que cumplen con un perfil profesional relacionado al ámbito de la seguridad de la información y otros profesionales de informática que sus tareas o labores diarias los han llevado a relacionarse con esta misma área.

3.6 Instrumentos de recolección de datos

En este caso tampoco es necesario aplicar o utilizar instrumentos de recolección de datos, dado que no es aplicable ningún estudio que contemple la recolección de datos para su posterior estudio.

Lepkowski (citado por Sampieri et al. 2014: 174) define: "… una población es el conjunto de todos los casos que concuerdan con una serie de especificaciones".

Para obtener datos desde diferentes fuentes de información, para llevar a cabo el proceso investigativo y el proceso de las encuestas; estas mismas se aplicarán a profesionales de la informática que tengan roles o sus labores estén relacionadas al ámbito de la seguridad de la información, con el fin de recolectar datos e información que coadyuve a obtener datos más exactos para la investigación.

3.7 Técnicas de análisis de información

Dado que no se van a recolectar datos, tampoco es necesario aplicar técnicas de análisis de información ya que no se aplica a un estudio que requiera este tipo de técnicas.

i. Instrumentos

1. Cuestionarios

Según Chasteauneuf (citado por Sampieri et al. (2014: 105)), el cuestionario es lo siguiente: "… conjunto de preguntas respecto de una o más variables a medir…" (p.217). Según Brace (citado por Sampieri et al. (2014: 105)): "Debe ser congruente con el planteamiento del problema e hipótesis" (p.217).

Dado que la información que se requiere recopilar debe provenir de distintos participantes o involucrados, se aplicará un cuestionario de siete preguntas para obtener todas las respuestas que coadyuven a un mayor conocimiento sobre la realidad del problema planteado y de esta manera lograr una propuesta que mejor se adapte a dichas necesidades.

Además, dado que se desea aplicar el cuestionario a un gran número de participantes de distintas ramas, se planea realizar dichos cuestionarios con cinco preguntas cerradas y dos abiertas, donde no solo el análisis de estas se

logre de manera rápida, sino que a la vez es más cómodo para los involucrados en las entrevistas responder las preguntas.

Según Sampieri et al. (2014: 105):

> Las preguntas cerradas contienen categorías u opciones de respuesta que han sido previamente delimitadas. Es decir, se presentan las posibilidades de respuesta a los participantes, quienes deben acortarse a éstas. Pueden ser dicotómicos (dos posibilidades de respuesta) o incluir varias opciones de respuesta.

Además,

> Las preguntas cerradas son más fáciles de codificar y preparar para su análisis. Asimismo, estas preguntas requieren un menor esfuerzo por parte de los encuestados, que no tienen que escribir o verbalizar pensamientos, sino únicamente seleccionar la alternativa que sintetice mejor su respuesta. Responder un cuestionario con preguntas cerradas toma menos tiempo que contestar uno con preguntas abiertas. Cuando el cuestionario se envía por correo, se tiene un mayor grado de respuesta porque es fácil de contestar y completarlo requiere menos tiempo. Otras ventajas son: se reduce la ambigüedad de las respuestas y se favorecen las comparaciones entre las respuestas (Burnett, 2009).

Capítulo 4. Análisis del diagnóstico

En este capítulo se exponen los resultados de los instrumentos de investigación aplicados con el fin de realizar un análisis que permita llevar a cabo el cumplimiento de los objetivos planteados en la investigación.

Los resultados se obtuvieron a partir de la participación de diferentes profesionales que mantienen una estrecha relación con el área de ciberseguridad

dado que los mismos actualmente laboran en empresas que aplican ciberseguridad, o bien, participan en estudios o investigación relacionada a esta área.

Con estos resultados, se pretende realizar un diagnóstico que sirva como base fundamental para lograr identificar problemas más específicos y reales de las organizaciones con los cuales se pueda desarrollar una estrategia que aplique diferentes posibles soluciones a dichos problemas.

a. Resultados de las encuestas

En la tabla 13 se muestran las preguntas que se realizaron en la encuesta diseñada para los profesionales.

Tabla 13: *Preguntas formuladas*

Número de pregunta	Pregunta	Opciones	Tipo de pregunta
1	¿Conoce o ha escuchado mencionar sobre la metodología Kill Chain?	• Sí • No	Cerrada
2	¿Conoce cómo se aplica dicha metodología en un modelo de SOC?	• Sí • No	Cerrada
3	¿Su empresa utiliza o ha implementado Kill Chain para atender incidentes de seguridad?	• Sí • No	Cerrada
4	¿Ha escuchado mencionar sobre la implementación de esta metodología en otras empresas?	• Ninguna • Algunas • Muchas	Cerrada

Número de pregunta	Pregunta	Opciones	Tipo de pregunta
5	¿Qué beneficios tiene utilizar Kill Chain?	No Aplica	Abierta
6	¿Qué cosas cambiaría sobre esta metodología?	No Aplica	Abierta
7	¿Es aconsejable implementarlo solo o con otras metodologías?	• Solo • Aplicando otras metodologías	Cerrada

Fuente: Elaboración propia.

En la tabla 14 se presentan las respuestas que se obtuvieran luego de haber aplicado la encuesta.

Tabla 14: *Respuestas obtenidas*

Pregunta 1	Pregunta 2	Pregunta 3	Pregunta 4	Pregunta 5	Pregunta 6	Pregunta 7
No.	No.	No.	Ninguna.			
No.	No.	No.	Ninguna.	No sé.	No sé.	Aplicando otras metodologías.
Sí.	No.	No.	Ninguna.	La mejora de capa una de las capas de seguridad.	De momento nada.	Aplicando otras metodologías.

Pregunta 1	Pregunta 2	Pregunta 3	Pregunta 4	Pregunta 5	Pregunta 6	Pregunta 7
Sí.	Sí.	Sí.	Algunas.	Detener de forma efectiva un ataque lo antes posible.	El concepto es en realidad muy similar a una metodología de ataque y a un modelo de defensa en profundidad, en términos generales no cambiaría nada.	Aplicando otras metodologías.
Sí.	No.	No.	Algunas.			Aplicando otras metodologías.
No.	No.	No.	Algunas.			
No.	No.	No.	Ninguna.			
Sí.	Sí.	Sí.	Ninguna.	Mejor comprensión del ataque.	N/A.	Aplicando otras metodologías.
Sí.	No.	No.	Ninguna.			Aplicando otras metodologías.
Sí.	Sí.	Sí.	Algunas.	Estandarización, orden y probabilidad.	Flexibilidad.	Aplicando otras metodologías.
Sí.	No.	No.	Ninguna.	No sé	No sé.	
No.	No.	No.	Ninguna.	NR.	NR.	Aplicando otras metodologías.
Sí.	No.	No.	Ninguna.			

Pregunta 1	Pregunta 2	Pregunta 3	Pregunta 4	Pregunta 5	Pregunta 6	Pregunta 7
No.	No.	No.	Ninguna.			
No.	No.	No.	Ninguna.			Aplicando otras metodologías.
No.	No.	No.	Ninguna.			Aplicando otras metodologías.
No.	No.	No.	Ninguna.			Aplicando otras metodologías.
No.	No.	No.	Ninguna.			Aplicando otras metodologías.
No.	No.	No.	Algunas.			

Fuente: Elaboración propia.

b. Análisis de las encuestas

Pregunta 1.

Se observa en la figura 14, que algunos profesionales, que representa el 57,9% de los encuestados, conocen o han escuchado sobre la metodología Kill Chain, mientras que hubo un 42,1% que no conoce o ha escuchado sobre esta metodología. Esto evidencia que la mayoría de los profesionales encuestados tienen alguna noción sobre el tema, lo que a su vez demuestra que muy posiblemente existan organizaciones con procesos de ciberseguridad donde se consulta la metodología, o se usa de referencia para las operaciones técnicas de la ciberseguridad.

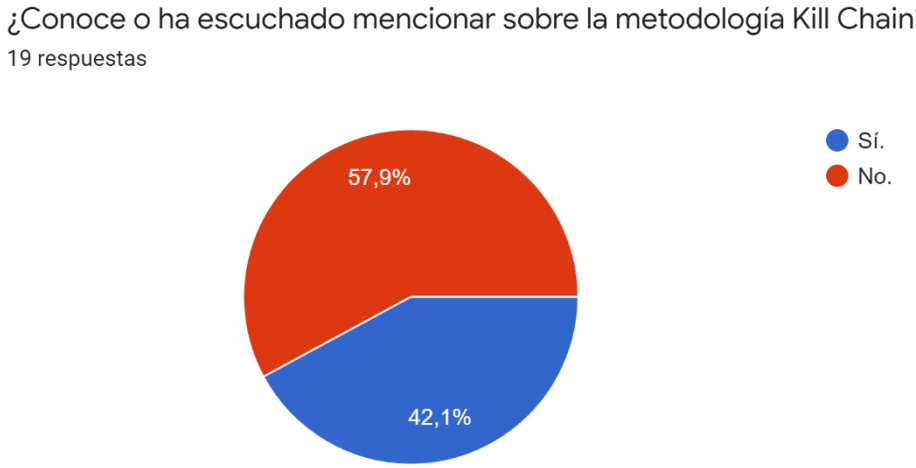


Figura 14: Gráfico pregunta 1. Fuente: Elaboración propia.

Pregunta 2.

En la figura 15 se observa que el 84,2% de los profesionales que participó en la encuesta, no conoce cómo se aplica dicha metodología en un servicio de SOC, mientras que el 15,8% sí tiene el conocimiento. Esto quiere decir que la gran mayoría de los participantes desconocen cómo aplicar la metodología en aquellos servicios de ciberseguridad que facilitan la identificación de ofensas cibernéticas, donde es requerido usar para una mejor trazabilidad del adversario y comprensión de sus técnicas de ataque la metodología Cyber Kill Chain.

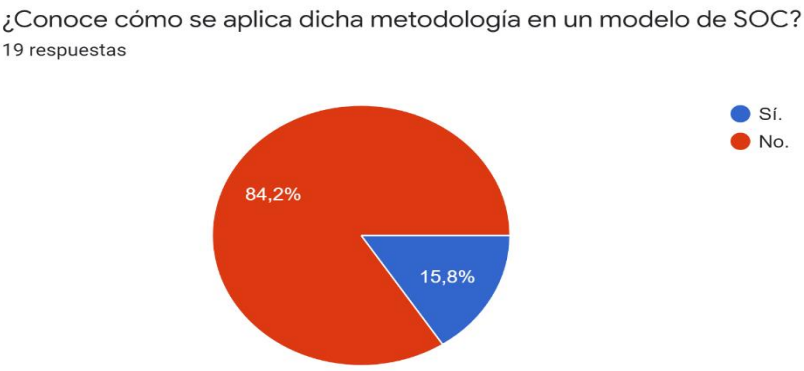


Figura 15: Gráfico pregunta 2. Fuente: Elaboración propia.

Pregunta 3.

Se muestra que el 84,2% de las empresas en la que laboran los profesionales encuestados, no han utilizado o han implementado Kill Chain para atender incidentes de seguridad, mientras que el 15,8% sí han utilizado o implementado la Kill Chain. Esto demuestra que muchas empresas requieren de mucho más tiempo de investigación para determinar la causa raíz de los ataques cibernéticos contra sus tecnologías, así mismo demuestra, una pobre comprensión del riesgo y la amenaza que atenta contra sus activos más críticos, provocando mayor tiempo de intervención del incidente y mayor tiempo de no operación de los servicios tecnológicos víctimas de ciber ataque, tal como se muestra en la figura 16.

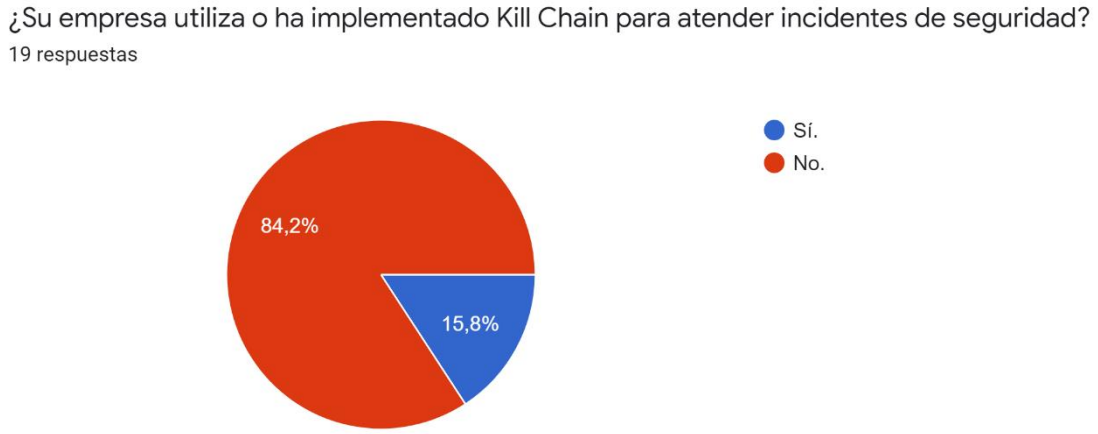


Figura 16: Gráfico pregunta 3. Fuente: Elaboración propia.

Pregunta 4.

Se muestra en la figura 17 que el 73,7% de los profesionales, no han escuchado mencionar sobre la implementación de esta metodología en otras empresas, mientras que el 26,3% opinan que solo algunas lo han hecho. Los resultados demuestran que muchas empresas todavía no utilizan este modelo, posiblemente utilizan otros o del todo no lo aplican.

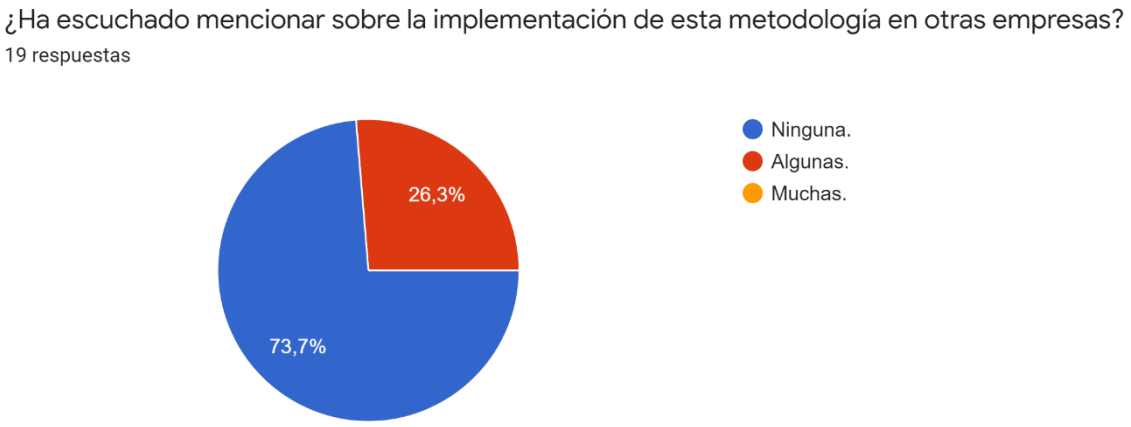


Figura 17: Gráfico pregunta 4. Fuente: Elaboración propia.

Pregunta 5.

Se muestra que existieron diferentes opiniones con respecto a los beneficios que existen al utilizar Cyber Kill Chain. Cabe señalar que esta pregunta únicamente fue respondida por aquellos participantes que han aplicado o utilizado la metodología, por lo cual se consideran las respuestas más sobresalientes. A continuación, se listan las mismas:

- “La mejora de una capa de las capas de seguridad”.
- “Detener de forma efectiva un ataque lo antes posible”.
- “Mejor comprensión del ataque”.
- “Estandarización, orden y probabilidad”.

Pregunta 6.

Se muestra que existieron diferentes opiniones con respecto a qué cosas cambiaría sobre esta metodología. Cabe señalar que esta pregunta únicamente fue respondida por aquellos participantes que han aplicado o utilizado la metodología, por lo cual se consideran las respuestas más sobresalientes. A continuación, se listan las mismas:

- “De momento nada”.

- “El concepto es en realidad muy similar a una metodología de ataque y a un modelo de defensa en profundidad, en términos generales no cambiaría nada”.
- “Flexibilidad”.
- “Estandarización, orden y probabilidad”.

Pregunta 7.

Esta pregunta fue respondida únicamente por aquellos participantes que han aplicado o utilizado la metodología, por lo cual el 100% de este análisis se refiere al 60% - 70% del total de los encuestados. Se observa que el 100% de los profesionales aconsejan implementar la metodología utilizando a su vez otras metodologías, tal como aparece en la figura 18.

Figura 18: Gráfico pregunta 7. Fuente: Elaboración propia.

Capítulo 5. Propuesta de solución

Evaluación de aplicabilidad del moldelo Cyber Kill Chain.

Es importante para cualquier empresa, sin importar su tamaño, ya sea pequeña, mediana o grande, proteger uno de los activos más importantes: la información. Es conocido que muchas empresas han sido afectadas por ataques del tipo APT en todo el mundo y las empresas en Costa Rica no están exentas de este tipo de ataques, dado que normalmente los objetivos de estos ataques se centran más en organizaciones y países de todo el mundo. Una de las cualidades más importantes de este tipo de ataques es que buscan obtener acceso a la red corporativa y una vez logrado este objetivo, la finalidad del ataque será mantener el acceso a este a largo plazo con la mayor discrecionalidad posible manteniendo como objetivo principal el robo o la destrucción de datos. Como ya es conocido, existen diferentes grupos APTs, así como amenazas no conocidas relacionadas al ámbito de los APTs, los cuales buscan afectar a las organizaciones de diferentes maneras. Por ejemplo, hay ataques que lo que buscan es el robo de información de la organización y otros que buscarán solo destruir la información.

Cabe señalar, que con el pasar del tiempo, las organizaciones y los gobiernos de diferentes países han ido fortaleciendo sus defensas frente a este tipo de ataques, dado que estos mismo poseen el financiamiento disponible para invertir en diferentes herramientas y soluciones de ciberseguridad, para la protección y el resguardo de la información. Más no así las pequeñas y las medianas empresas, pues no poseen suficiente capital como para invertir en soluciones tan sofisticadas, por lo cual los ataques APTs se han orientado a este tipo de organizaciones, las cuales en muchos casos no cuentan ni si quiera con un plan de seguridad para la protección de la información. Considerando la encuesta aplicada, se conoce que, en algunas organizaciones, incluyendo grandes compañías, no han escuchado mencionar el marco de trabajo de Cyber Kill Chain, el cual es conocido como uno de los marcos de trabajo que mejor se orienta para la defensa contra amenazas persistentes avanzadas. El resultado ha demostrado ser preocupante, dado que conforme siguen existiendo avances tecnológicos en diferentes ámbitos, estos tipos de ataques se sofisticando y especializando más, dando como resultado una mayor brecha de seguridad en las organizaciones que no contemplan o no invierten en planes de seguridad orientados a la mitigación de este tipo de ataques.

El marco de trabajo de Cyber Kill Chain ofrece una visión holística sobre una serie de eventos o cadena de ataques que conforman un APT. Por esto mismo aplicando este marco de trabajo, la organización puede analizar los ataques APT conociendo la cadena de sucesos que dan lugar al ataque en su completitud; sin embargo, uno de los objetivos principales de este marco de trabajo es detectar y detener el ataque lo más antes posible, con el fin de reducir los riesgos que se puedan materializar a causa del mismo ataque. Cyber Kill Chain se considera como parte de una estrategia de Inteligencia de Amenazas, donde, primero se debe recopilar la información sobre los eventos o sucesos que estén aconteciendo para luego analizar y aplicar las medidas correspondientes, así como para dar una mejor respuesta ante el ataque. Cabe señalar que Cyber Kill Chain puede ser aplicado a cualquier tipo de ataque; sin embargo, su principal uso se orienta a la detección de ataques de mayor complejidad o de los cuales no se tiene conocimiento alguno y en donde se debe de actuar lo más antes posible.

Dependiendo de la organización, puede utilizar o aplicar este marco de trabajo con otros, tal como MITRE ATT&CK con el fin de reforzar las medidas de seguridad de la organización, o bien, como un complemento a su estrategia actual de ciberseguridad. Es importante reconocer a nivel de la organización el estado de seguridad de la información a través de distintos mecanismos como puede ser el uso de un modelo de madurez de seguridad que demuestre que en la organización se están aplicando las medidas correspondientes, o bien, que con los mecanismos de protección existentes no se estén cubriendo ciertos tipos de amenazas, en especial, las amenazas persistentes avanzadas.

A continuación, en la figura 19 se muestran las fases de Cyber Kill Chain.

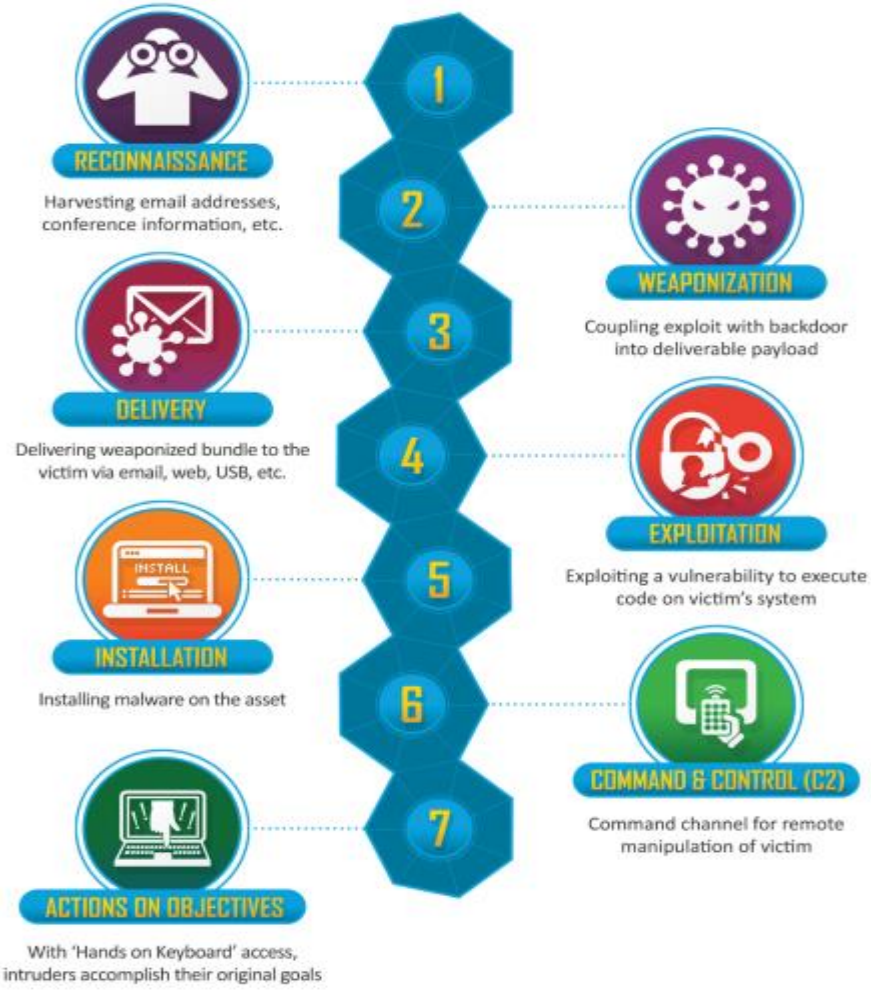


Figura 19: Fases de Cyber Kill Chain. Fuente: Disponible en https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Como se aprecia, el marco de trabajo ofrece siete fases que normalmente se dan cuando ocurre un ataque.

1. Reconocimiento. En esta fase, los atacantes buscan información relevante sobre vulnerabilidades que puedan explotar de la organización a través de la identificación de servicios y aplicaciones activas. El atacante podría realizar el proceso sobre esta fase, ya sea de forma pasiva, donde buscará obtener información de fuentes abiertas o información de la organización que se encuentre disponible en internet sin la necesidad de corromper ningún sistema; o bien, puede que lo haga de forma activa, donde trate de obtener la información a través de los sistemas de la organización.

2. Armamento. Se determina cómo se realizará el ataque. Como parte de la planificación el atacante podría tratar de ocultar una carga útil maliciosa como una aplicación empresarial o un tipo de archivo del sistema operativo que es fácilmente ejecutable en los sistemas operativos, dado que se pueden llegar a reconocer como archivos ejecutables, documentos en diferentes formatos, scripts o cargas útiles de manipulación de códigos de shell.
3. Entrega. Para la fase de entrega, se busca enviar el payload o el malware utilizando la ingeniería social en donde el atacante envía correos electrónicos falsos, sirve sitios web falsos o de alguna forma inserta malware a través de un dispositivo usb.
4. Explotación. En esta fase es donde realmente inicia el ataque.
5. Instalación. Después de haber iniciado el ataque, el atacante trata de generar persistencia, por lo cual el malware utilizado se mantiene en ejecución aun después de haber apagado o reiniciado el equipo de la víctima.
6. Comando y Control. Una vez instalado el malware en un equipo de la organización y generando persistencia, el payload o carga útil se conecta con el atacante para recibir más instrucciones, realizar más manipulaciones, exfiltrar información de credenciales, entre otros.
7. Acciones sobre objetivos. En esta última fase, el atacante logra el control del sistema, por lo cual puede moverse lateralmente por la red interna de la organización y recolectar información por un largo período de tiempo sin ser detectado.

A continuación, en la figura 20 se muestra un modelo de amenazas persistentes avanzadas y su ciclo de vida.

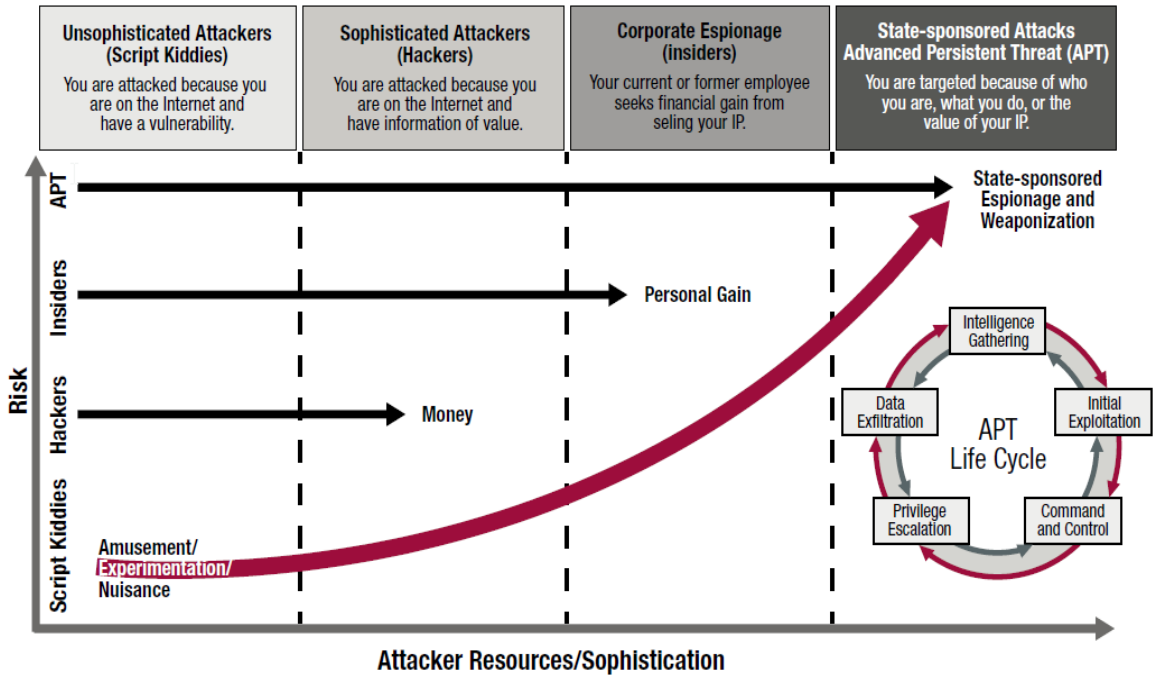


Figura 20: Modelo de amenazas persistentes avanzadas y su ciclo de vida. Disponible en http://drshem.com/2015/10/08/cybersecurity-origins-of-the-advanced-persistent-threat-apt/

Como se muestra, según el modelo evolutivo de amenazas persistentes avanzadas y su ciclo de vida, existen diferentes etapas que podrían llegar a darse dependiendo del tipo de atacante. En este caso, se consideran los Script Kiddies, quienes pueden estar motivados a realizar un ataque a la organización por diversión, por experimentar o por causar molestia. Los Script Kiddies se consideran muy peligrosos, puesto que por su mismo desconocimiento pueden llegar a causar grandes fallas que ni ellos mismos podrían llegar a controlar, pues incluso pueden utilizar malware o técnicas sofisticadas a través de herramientas desarrolladas por hackers sofisticados. Se puede ser víctima de un Script Kiddie si la organización es rastreable en la red y además mantiene vulnerabilidades en los sistemas.

Continuando con el proceso del modelo, los ataques sofisticados se dan por Hackers, quienes han logrado rastrear la organización y además tienen información muy importante con la cual pueden llevar a cabo diferentes tipos de ataques. Cabe señalar que la motivación de los hackers es el dinero, aunque dependiendo no siempre es así dado que podrían estar motivados por otros factores.

Luego se encuentran los Insiders, quienes están motivados por beneficios personales y que buscan un beneficio, ya sea económico, o incluso quieran solamente deseen dañar a la organización de alguna forma. Es importante resaltar que normalmente a quienes se les conoce como Insiders son los mismos empleados de la organización; sin embargo, hay que recordar que, si un atacante externo logra infiltrarse en la red corporativa, este puede llegar a ser un Insider, dado que ya se encuentra dentro de la red, donde incluso, puede llegar a obtener credenciales de otros empleados; o bien, él mismo puede pasar desapercibido en la red como un usuario más con credenciales de la organización.

Por último, se encuentran las amenazas persistentes avanzadas, que son ataques mucho más sofisticados, dado que se cuenta con el patrocinio de diferentes grupos de interés, los cuales tienen una alta capacidad para financiar los ataques. Estos ataques pueden estar motivados por diferentes aspectos, pero uno de los principales es el espionaje.

Las amenazas persistentes avanzadas cuentan con su propio ciclo de vida, donde se identifican etapas como: la obtención de información, explotación inicial, comando y control, escalación de privilegios y exfiltración de datos; por lo cual se logra demostrar que estas etapas son muy similares a las fases que sigue el marco de trabajo de Cyber Kill Chain. Considerando la similitud entre las distintas etapas, la organización puede identificar que el marco de trabajo de Cyber Kill Chain se adapta muy bien al ciclo de vida de las amenazas persistentes avanzadas, con lo cual se puede servir de este instrumento como parte del proceso de evaluación de aplicabilidad. Para esto, la organización también debe considerar si existen vulnerabilidades con respecto a cada una de las etapas identificadas.

Como parte de la solución, se desarrollan una serie de etapas, las cuales se deberán de seguir para evaluar la aplicabilidad del marco de trabajo de Cyber Kill Chain. Para esto, se define un instrumento de evaluación, el cual pueda servir como una herramienta para el profesional en seguridad de la información o los encargados en implementar la estrategia de seguridad en la organización.

1. Etapa de reconocimiento.

   En la etapa de reconocimiento, el profesional encargado de realizar la evaluación de aplicabilidad del marco de trabajo de Cyber Kill Chain deberá obtener la información completa sobre todos los equipos y tecnologías utilizadas en la infraestructura hacia la cual se pretende aplicar dicho marco de

trabajo, con el fin de reconocer cuales equipos y tecnologías son las que se deberían de evaluar o tener una base sobre la cual comenzar a realizar el proceso de evaluación. En este caso, el profesional deberá llevar a cabo una Evaluación de Activos de TI, en el cual se pueda dar la mayor trazabilidad posible sobre la infraestructura crítica de la organización.

Para esto, el encargado de realizar la evaluación puede establecer un documento en el cual se enlisten los activos identificados; o bien, si la organización ya cuenta con un sistema para realizar dicho proceso eventualmente deberá de solicitar la información al equipo encargado de gestionarla.

2. Etapa de diagnóstico.

   Una vez que se hayan recabado los datos, el profesional puede analizar el estado actual de la seguridad de los equipos y las tecnologías que se han implementado o que forman parte de la infraestructura crítica de la organización. Para esto, también se puede aplicar un proceso de evaluación de vulnerabilidades, con el fin de obtener todas aquellas vulnerabilidades existentes y las cuales posteriormente podrían ser cubiertas con un marco de trabajo de Cyber Kill Chain.

3. Etapa de análisis.

   En la etapa de análisis, se examinan qué herramientas o soluciones de seguridad se han implementado en cada uno de los equipos o tecnologías identificadas para a su vez identificar debilidades a nivel de acceso, procesos de monitoreo de identidad, tanto de equipos como de usuarios, soluciones de automatización de seguridad de la información y herramientas analíticas para la evaluación de datos que demuestren con exactitud Indicadores de Compromiso (IoCs) y otra información que sea relevante al momento de detectar y tratar las diferentes amenazas que se puedan presentar.

   Cabe señalar, que esta etapa es muy importante para que el profesional encargado de realizar la evaluación tenga una base sobre la cual pueda responder a diferentes cuestiones planteadas en el instrumento de evaluación de aplicabilidad de Cyber Kill Chain, el cual es utilizado en la siguiente etapa.

4. Etapa de implementación.

   En esta etapa, es donde se implementa el instrumento de evaluación de aplicabilidad de Cyber Kill Chain, el cual a su vez se sigue un proceso

estructurado también por etapas con el fin de obtener los resultados de la evaluación de manera exacta.

A continuación, se muestra y se explican cada una de las etapas a seguir en el instrumento de evaluación de aplicabilidad del marco de trabajo de Cyber Kill Chain:

1. Etapa de definición de niveles.

En esta etapa, se definen los niveles que establecen los diferentes parámetros para realizar el proceso de evaluación. Estos niveles se establecen de la siguiente manera:

Cuantitativamente, se refieren a los parámetros numéricos que se utilizarán como referencia para aplicar distintas medidas estadísticas a partir con base de los resultados que se vayan obteniendo del cuestionario.

Cualitativamente, se refieren al significado de cada uno de los parámetros numéricos de forma cualitativa, por lo cual se describen cada uno de ellos.

Es importante destacar, que los parámetros numéricos se utilizan para aplicar diferentes cálculos que demuestren el nivel de implementación de Cyber Kill Chain, con los cuales se pueda generar datos estadísticos que sirvan para la generación de gráficos y de esta manera obtener una visualización más exacta y sencilla de los resultados. Sin embargo, estos parámetros también tienen su propia descripción con el fin de obtener resultados que se puedan analizar de manera cualitativa de tal manera que faciliten expresar los resultados obtenidos descriptivamente.

Según lo establecido en el instrumento de evaluación se define lo siguiente:

Tabla 15: *Nivel de implementación Cyber Kill Chain*

Nivel de Implementación Cyber Kill Chain		
0	Inexistente	La fase o la etapa no se ha aplicado y no existe ninguna estrategia relacionada que se haya aplicado
1	Inicial	La fase o la etapa ha sido considerada por la organización por lo que se encuentra en un etapa inicial, sin embargo, no se ha comenzado a desarrollar
2	En proceso	La fase o la etapa se encuentra en un proceso de desarrollo
3	Implementado	La fase o la etapa se ha logrado implementar, sin embargo, no se ha desarrollado y no ha a alcanzado un nivel de madurez alto
4	Avanzado	La fase o la etapa ha logrado alcanzar cierto nivel de madurez con respecto a su implementación, sin embargo, no ha alcanzado su nivel máximo
5	Completado	La fase ola etapa se ha logrado implementar en su completitud

Fuente: Elaboración propia.

2. Etapa de análisis.

En esta etapa, el profesional encargado de aplicar el instrumento de evaluación deberá responder a una serie de preguntas formuladas con las cuales se busca detectar si las diferentes fases de Cyber Kill Chain están cubiertas por la organización. Para esto, se establece una estructura que considere también las etapas existentes en Cyber Kill Chain, las cuales son pre-compromiso, compromiso y post compromiso. A cada una de estas etapas corresponde una serie de fases de Cyber Kill Chain, las cuales son reconocimiento, preparación, distribución, explotación, instalación, comando y control, y acciones sobre objetivos. En la tabla 16 se muestra cómo estas etapas y fases están ordenadas, así como también las preguntas que corresponden a cada una de las fases y las respuestas, las cuales deberán ser respondidas por el encargado de realizar el proceso de evaluación.

Tabla 16: *Análisis nivel de implementación Cyber Kill Chain*

Análisis Nivel de Implementación Cyber Kill Chain

Etapas y Fases	Preguntas	Respuestas	
Etapa de pre compromiso		Sí	No
Reconocimiento	¿Existen mecanismos para la protección de información pública de la organización que pueda revelar datos confidenciales?		x
	¿Existen mecanismos para el control de perfiles completos sobre la organización en la	x	
	¿Existe información confidencial expuesta al público?	x	
	¿La información de los sistemas que componen la infraestructura de TI de la organización es díficil de obtener?		x
	¿Existen mecanismos de control para la protección de los nombres de dominio?		x
	¿Los sitios web de la empresa implementan mecanismos de seguridad?	x	
	¿Los puertos de los diferentes servidores y sistemas están protegidos?		x
	¿Existen mecanismos control de anti spam?		x
	¿La organización implementa políticas para mitigar o evitar el phishing?	x	
	¿La organización implementa controles de seguridad orientados a la ingeniería social?		x
	¿La organización implementa mecanismos de analítica web?		x
	¿La organización implementa políticas orientadas a la regulación de la información que se publica en la web?	x	
	¿La organización implementa firewalls en su infraestructura?		x
	¿La organización implementa sistemas de prevención intrusiones?		x
	¿La organización implementa mecanismos de autenticación?	x	
	¿Existen políticas de control sobre el uso de las redes sociales?		x
	¿En caso de publicarse información que debe mantenerse pública, se aplican métodos de cifrado de la información para impedir accesos no autorizados?	x	
	¿En caso de utilizar servicios públicos en la nube, la información que maneja está protegida, o bien, es información que no revela datos importantes sobre la compañía?		x
	¿La organización implementa mecanismos orientados a proteger perímetro más externo de la red?	x	
	¿La organización conoce todos los puntos de entrada de los diferentes sistemas?		x
Preparación	¿La organización implementa mecanismos de control y trazabilidad de puertas traseras?		x
	¿La organización implementa mecanismos de control y trazabilidad para el acceso remoto?	x	
Distribución	¿La organización implementa un programa de concientización sobre ingeniería social?		x
	¿La organización implementa sistemas de detección y de filtro de correos maliciosos?	x	
	¿La información de los empleados no se encuentra expuesta como para recibir información que no sea de competencia para la compañía?		x
	¿La información de identidad de los usuarios o empleados se encuentra protegida?		x
	¿Existen datos de la organización que puedan ser difícilmente enmascarados?	x	
	¿Se implementa algún mecanismo de control para evitar el enmascaramiento de datos o información de la organización?		x
	¿Existen mecanismos para contrarrestar la descarga de archivos, en cualquier formato existente, no autorizados o sospechosos?	x	
	¿Existen mecanismos o medidas para la protección de los medios físicos usb?		x
	¿Se implementan mecasnimos para evitar o contrarrestar vulnerabilidades a nivel de DNS?	x	
	¿Se implementan mecanismos de captura de paquetes para el análisis de red?		x
	¿Existe un control exhaustivo sobre el tráfico de red de la organización?		x
	¿Existen metodos para medir los niveles de implementacion de los programas de concientización?	x	

Etapa de compromiso			
Explotación	¿Los sistemas operativos y el software que se utiliza en la organización son seguros?		x
	¿Los sistemas operativos y el software que se utiliza en la organización son debidamente mantenidos?	x	
	¿Se implementa software anti virus en los diferentes equipos de los empleados?		x
	¿Existen mecanismos de control para el acceso remoto por medio de consola?		x
	¿La organización cuenta con mecanismos de seguridad para exploits?	x	
	¿La organización cuenta con mecanismos de seguridad para ataques de denegación de servicios?		x
	¿La organización cuenta con mecanismos de seguridad para la protección de explotaciones a nivel de protocolos (FTP, SMTP, NTP, SSH, entre otros)?		x
	¿La organización cuenta con mecanismos de seguridad contra ataques dirigidos a la administración de la memoria de los diferentes equipos?		x
	¿La organización cuenta con sistemas de detección de intrusos en la red?	x	
	¿Existen mecanismos para la detección de anomalías en los datos entrantes y salientes de la red de la organización?		x
	¿La organización da un seguimiento sobre las detecciones o monitores que se realizan a nivel de los sistemas?		x
	¿La organización hace uso de indicadores de compromiso así como de otros indicadores con el fin de mejorar el proceso de análisis en las detecciones y el monitoreo?		x
	¿La acciones de las detecciones o monitoreo que se realiza están automatizadas?	x	
	¿La organización implementa mecanismos de registro de logs de los diferentes sistemas?		x
	¿La organización implementa una política de retención de registros de logs?		x
	¿La organización implementa mecanismos para la correlación de eventos o registros logs?		x
Instalación	¿Existen controles de seguridad a nivel de los equipos de los usuarios que eviten la instalación ejecución de software malicioso?		x
	¿La configuración en los equipos evita que los usuarios, aplicaciones o servicios puedan ejecutar tareas sin autorización de la organización?		x
	¿Existen mecanismos de seguridad que eviten que se inicien aplicaciones o servicios de manera automática al iniciar los equipos de los usuarios o empleados?		x
	¿Existen mecanismos para el tratamiento de amenazas críticas como el ransomware?	x	
	¿Existen sistemas de respaldo que faciliten la recuperación de la información en caso de pérdida de la misma?		x
	¿Se realiza un análisis de malware en sospechas malware?	x	
Etapa de post compromiso			
Comando y control	¿Existen mecanismos de seguridad que eviten la exfiltración de la información de la organización?		x
	¿Existen mecanismos de control para evitar la comunicación de los sistemas de la organización con servidores externos maliciosos?	x	
	¿Existen mecanismos para interrumpir accesos o comunicaciones remotas no permitidas?		x
	¿Existen mecanismos para filtrar las direcciones IP y los protocolos HTTP?	x	
	¿Se implementan mecanimos de seguridad que permitan limitar las solicitudes HTTP?		x
	¿Existen mecanismos para detectar actividad inusual en las cuentas de los usuarios?		x
Acciones sobre objetivos	¿Los sistemas de la organización son interdependientes o se implementan mecanismos de seguridad que eviten ataques masivos sobre los distitntos sistemas de la organización?		x
	¿Existen mecanismos para evitar que los sitemas de la organización se puedan utilizar para ataques basados en botnets?	x	
	¿Existen controles que eviten el control directo sobre los diferentes equipos o sistemas de la organización?	x	
	¿Las credenciales de los sistemas y de los usuarios están debidamente protegidas?		x
	¿Se implementan sistemas de seguridad que permitan la detección o revisión de proxies?	x	
	¿Se implementan firewalls basados en lista de control de acceso?		x
	¿Se implementa una infraestructura basada en honeypots?		x

Fuente: Elaboración propia.

Como parte del proceso de análisis, se incorporan las estadísticas de cada una de las fases, así como las de cada una de las etapas. En las estadísticas de las fases, se establece una tabla en la cual se visualizan los resultados numéricos. Estos servirán para analizar los resultados con una perspectiva cuantitativa y además para la generación de gráficos, así como para la obtención de resultados que se utilizarán, tanto en las estadísticas de las etapas, como en los resultados finales del instrumento de evaluación.

En la tabla 17 se establecen cuatro distintas columnas. En la primera columna, se enlistan las fases, las cuales a su vez consideran el resultado promedio obtenido, tanto de las respuestas afirmativas como de las negativas. La segunda columna enlista el total de preguntas que corresponden a cada una de las fases. La tercera columna corresponde al total de respuestas afirmativas obtenidas. Cabe señalar que, los resultados promedios, así como el nivel de implementación con respecto a los distintos niveles establecidos, también se enlistan en esta columna, pero están descritos en la primera columna según corresponda. La cuarta columna corresponde al total de respuestas negativas obtenidas. En esta columna también se enlistan los resultados promedios, así como el nivel de implementación con respecto a los distintos niveles establecidos, pero también están descritos en la primera columna según corresponda.

Tabla 17: *Datos estadísticos de las fases*

Datos Estadísticos de las Fases			
Fases	Total Preguntas	Resultados Afirmativos	Resultados Negativos
Reconocimiento	20	8	12
Promedio Reconocimiento		0.4	0.6
Nivel de Implementación		2	3
Preparación	2	1	1
Promedio Preparación		0.5	0.5
Nivel de Implementación		2.5	2.5
Distribución	13	5	8
Promedio Distribución		0.38	0.62
Nivel de Implementación		1.9	3.1
Explotación	16	4	12
Promedio Explotación		0.25	0.75
Nivel de Implementación		1.25	3.75
Instalación	6	2	4
Promedio Instalación		0.33	0.67
Nivel de Implementación		1.65	3.35
Comando y control	6	2	4
Promedio Comando y control		0.33	0.67
Nivel de Implementación		1.65	3.35
Acciones sobre objetivos	7	3	4
Promedio Acciones sobre ob		0.43	0.57
Nivel de Implementación		2.15	2.85

Fuente: Elaboración propia.

Lo mismo aplica para la tabla 18 definida para las etapas.

Tabla 18: *Datos estadísticos de las fases*

Datos Estadísticos de las Etapas			
Etapas	Total Preguntas	Resultados Afirmativos	Resultados Negativos
Pre compromiso	35	14	21
Promedio Pre Compromiso		0.4	0.6
Nivel de Implementación		2	3
Compromiso	22	6	16
Promedio Compromiso		0.27	0.73
Nivel de Implementación		1.35	3.65
Post Compromiso	13	5	8
Promedio Post Compromiso		0.38	0.62
Nivel de Implementación		1.9	3.1

Fuente: Elaboración propia.

Cabe señalar, que las fórmulas que se presentan aplican para ambas tablas (17 y 18); sin embargo, lo único que cambia es la cantidad de los valores que se consideran para el análisis, pues las etapas consideran todas las preguntas y respuestas de las fases que formen parte de estas. En este sentido, los resultados de las etapas son más globales con respecto a las fases y los resultados de las fases que son más específicos por cada una de ellas.

A continuación, se muestran las fórmulas aplicadas para la generación de los datos numéricos en cada una de las columnas en la tabla:

- Número total de preguntas, resultados afirmativos y negativos: para definir el número total de preguntas establecidas en cada una de las fases y etapas se considera la sumatoria total de la cantidad de preguntas existentes en cada una de ellas. La fórmula utilizada es la siguiente:

$$\sum_{i=1}^{n} x_i$$

En donde:

n: Indica el límite superior. El valor que se le asigna es el total de elementos a contabilizar.

i: Indica el índice de la suma. El valor que se le asigna indica en donde comenzará la sumatoria hasta alcanzar el límite superior o el valor n.

x: Indica los valores que se van sumando.

Ejemplo:

n = 20

i = 1

X = 1

$$\sum_{i=1}^{20} X_i = 1_1 + 1_2 + \cdots = 20$$

Dado que se está trabajando con Excel, solo se consideran las celdas que tienen valores o que están llenas. No se cuentan los valores vacíos, por lo cual se utiliza la función de Excel “CONTARA” considerando el rango de celdas que pertenecen a sus respectivas columnas y cada una de las fases.

Cabe señalar que el total de preguntas que se obtiene por cada fase y etapa es solamente un valor que se utilizará para obtener los resultados promedios.

- Resultado promedio de los resultados afirmativos y negativos: para definir los resultados promedios de los resultados afirmativos y negativos según el total de preguntas existentes, se considera la siguiente formula:

  $$x = \frac{a}{b}$$

  En donde, en nuestro contexto:

  x: Indica el valor promedio de los resultados.

  a: Indica el total de los resultados de las respuestas.

  b: Indica el total de las preguntas.

  Considerándose la fórmula de la regla de tres, se aplican los cálculos necesarios. En este caso, se considera la regla de tres, sin embargo, no se aplica tal cual dado que se reajusta al problema específico en este contexto.

Dado que lo que se busca es obtener un valor que sea proporcional con respecto a la escala de los niveles, primero se debe obtener un valor promedio. Sin embargo, como los resultados de las respuestas dependen en gran medida de la cantidad total de las preguntas, se debe de dividir el valor total de las respuestas obtenidas entre el total de preguntas. En dado caso, para obtener el valor promedio de los resultados afirmativos y negativos se deben considerar el total de cada uno de ellos y dividirlos entre el total de preguntas según corresponda.

Ejemplo:

a = 8

b = 20

$$x = \frac{8}{20}$$

$$x = 0.4$$

El resultado final se debe obtener en valores decimales, puesto que luego se debe escalar a una menor proporción, en este caso, la escala definida por el valor máximo de los niveles el cual es 5. Por lo tanto, el dividendo debe ser el valor total de los resultados de las respuestas y el divisor debe ser el total de las preguntas.

- Resultado promedio de los valores afirmativos y negativos con respecto al nivel de implementación:

Para definir los resultados promedio de los valores afirmativos y negativos con respecto al nivel de implementación, se considera la siguiente formula:

$$x = a * b$$

En donde, en nuestro contexto:

x: Indica el valor promedio de los valores afirmativos y negativos con respecto al nivel de implementación.

a: Indica el valor promedio de los resultados obtenidos anteriormente. En este caso, el valor x de la formula anterior.

b: Indica el total o máximo de los niveles. Este es un valor 5 el cual es constante.

Dado que se debe realizar un cálculo para identificar la posición de los valores promedios obtenidos anteriormente según los niveles, se debe establecer una proporción entre el valor total de las preguntas, los cuales son variables dependiendo de la fase o etapa que se esté evaluando, con respecto, al valor total de los niveles el cual es un valor constante y conocido pues estos se conocen a razón de que se definieron los valores cuantitativos de los niveles. Por ende, el valor total de las preguntas es proporcional al valor total de los niveles, pues representan el valor máximo, que representa el 100% o el valor total, con el que se debe evaluar cada uno de los resultados afirmativos y negativos.

Ejemplo:

a = 0.4

b = 5

$$x = 0.4 * 5$$

$$x = 2$$

Este resultado final es el que se utilizará para conocer en qué nivel de implementación se encuentra cada fase o etapa de Cyber Kill Chain. Además, con los resultados obtenidos se generan los gráficos correspondientes a las fases y a las etapas.

A continuación, se presentan los gráficos de las fases, correspondientes a las figuras 21, 22, 23, 24, 25, 26, 27 y 28.

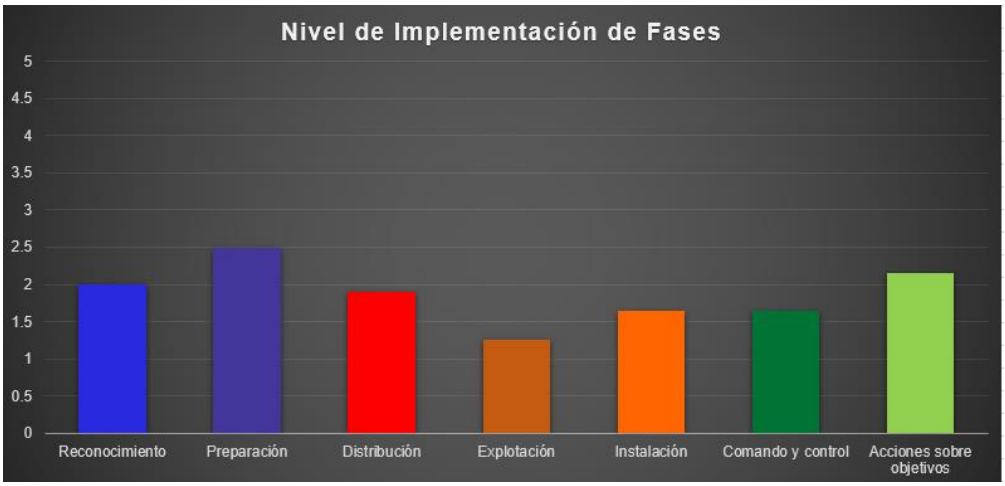


Figura 21: Nivel de implementación de fases. Fuente: Elaboración propia.

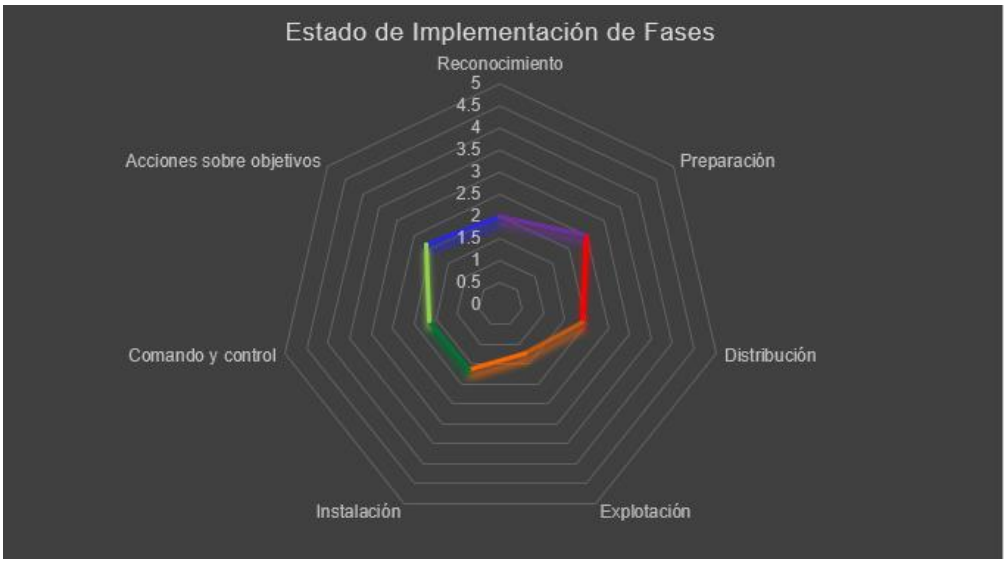


Figura 22: Estado de implementación de fases. Fuente: Elaboración propia.

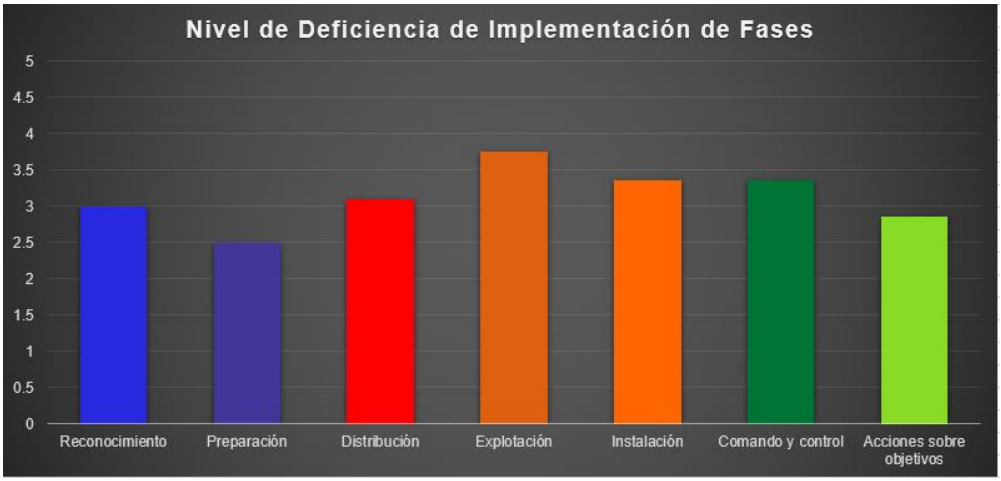


Figura 23: Nivel de deficiencia de implementación de fases. Fuente: Elaboración propia.

Figura 24: Estado de deficiencia de implementación de fases. Fuente: Elaboración propia.

A continuación, se presentan los gráficos de las etapas.

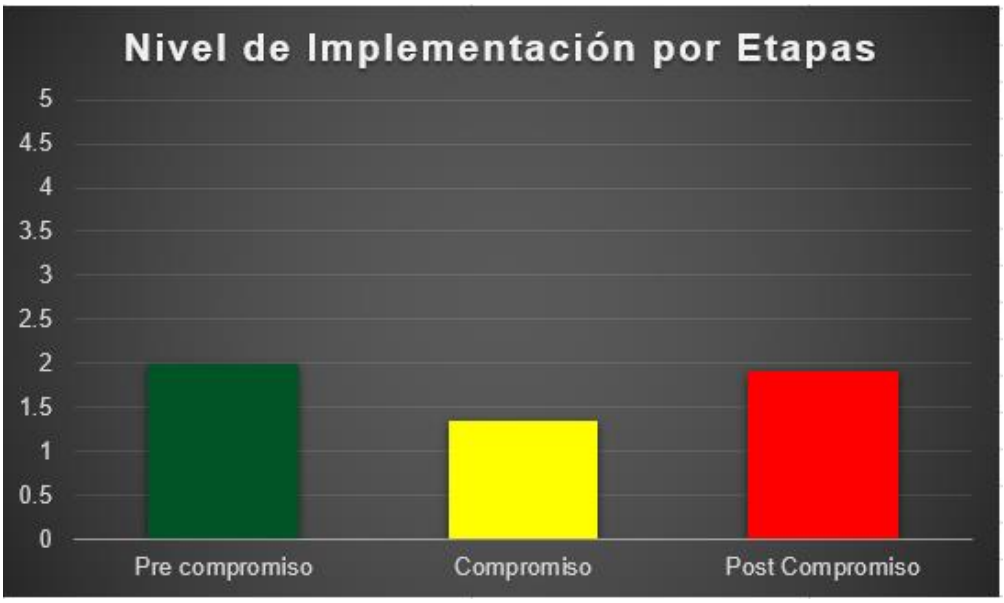


Figura 25: Nivel de implementación por etapas. Fuente: Elaboración propia.

Figura 26: Estado de implementación por etapas. Fuente: Elaboración propia.

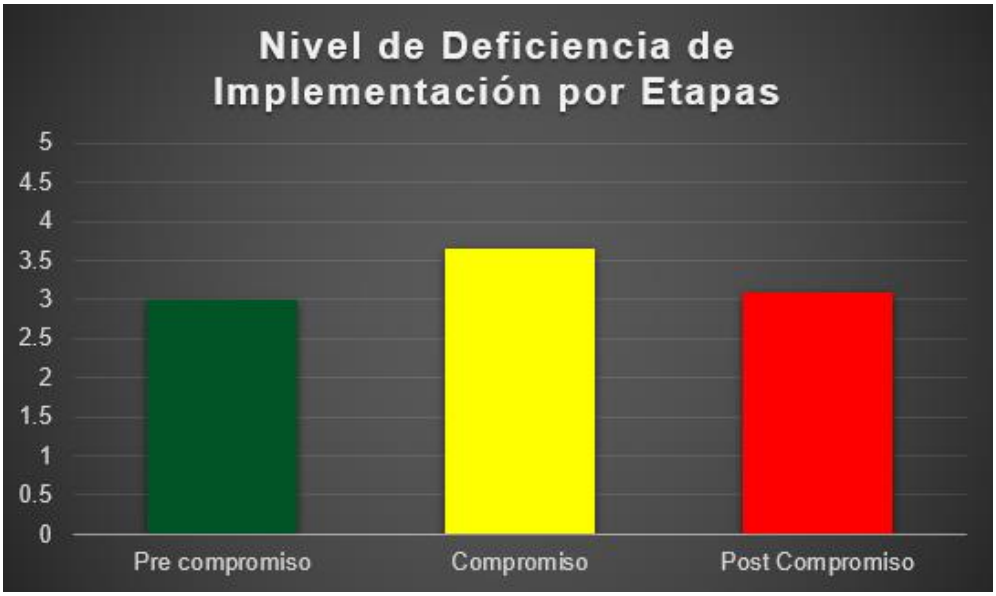


Figura 27: Nivel de deficiencia de implementación por etapas. Fuente: Elaboración propia.

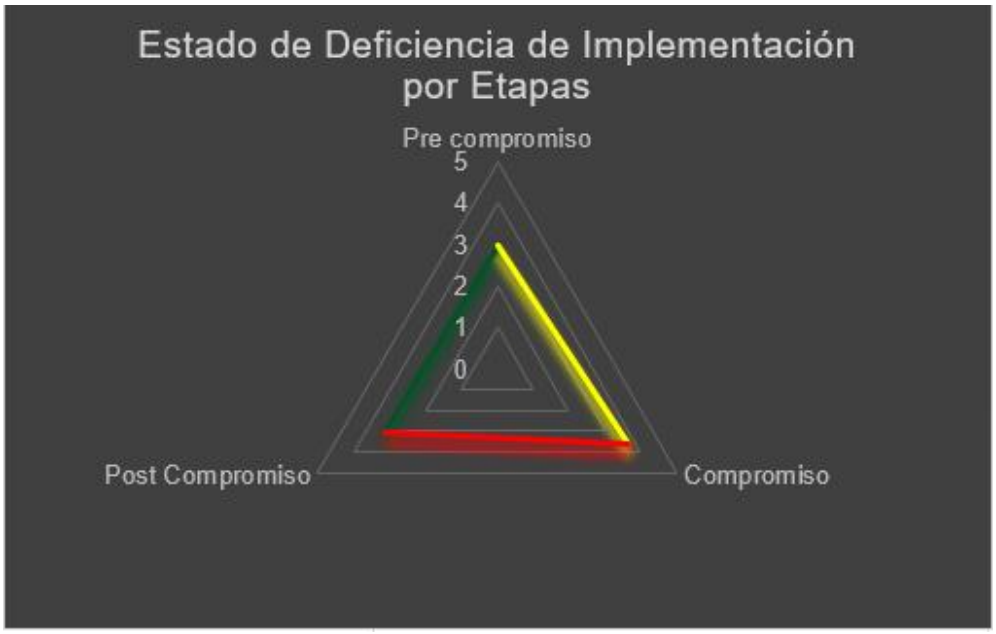


Figura 28: Estado de deficiencia de implementación por etapas. Fuente: Elaboración propia.

3. Etapa de resultados.

En esta etapa, el estratega evaluará los resultados finales del proceso de análisis, los cuales se muestran a partir de las tablas 19 y 20.

Tabla 19: *Análisis de implementación de Cyber Kill Chain*

Análisis Nivel de Implementación Cyber Kill Chain		
Etapas y Fases	Nivel de Implementación Positivo	Nivel de Implementación Negativo
Etapa de pre compromiso	2.05	2.95
Reconocimiento	2	3
Preparación	2.5	2.5
Distribución	2.1	2.9
Etapa de compromiso	1.35	3.65
Explotación	1.25	3.75
Instalación	1.65	3.35
Etapa de post compromiso	1.9	3.1
Comando y control	1.65	3.35
Acciones sobre objetivos	2.15	2.85

Fuente: Elaboración propia.

Tabla 20: *Niveles de implementación de Cyber Kill Chain*

Niveles de Implementación de Cyber Kill Chain	
Valores Cuantitativos	Valores Cualitativos
0	Inexistente
1	Inicial
2	En proceso
3	Implementado
4	Avanzado
5	Completado

Fuente: Elaboración propia.

Cabe señalar que estos resultados se generarán de manera automática según los resultados del cuestionario, así como según los resultados de los gráficos. El estratega logrará observar el estado cómo se ubican los diferentes niveles de implementación según cada una de las fases y de las etapas que comprende el marco

de trabajo de Cyber Kill Chain. Para esto, se considera la tabla de los niveles de implementación que muestra los valores cuantitativos y cualitativos. Los valores cuantitativos mostrarán en donde se ubican cada uno de los resultados obtenidos y los valores cualitativos muestran el estado de implementación en el que se encuentran. Con esto, se logrará tomar una decisión final sobre la implementación del marco de trabajo de Cyber Kill Chain para la organización.

5. Etapa de resultados.

   Una vez que se han logrado obtener los resultados finales del instrumento de evaluación, el analista procederá a analizar dichos resultados considerando las etapas de reconocimiento, diagnóstico, análisis e implementación; siendo la etapa de implementación donde mayormente obtendrá los datos y los resultados necesarios para tener un criterio más exacto. Con respecto a la etapa de implementación, el analista logrará servirse de los datos estadísticos, así como de los resultados finales que entrega el instrumento de evaluación, para definir si debe o no implementar el marco de trabajo de Cyber Kill Chain en su organización.

   Si el estratega desea continuar con la implementación del marco de trabajo de Cyber Kill Chain en su organización, se puede servir de la matriz de las vías de acción, como la presentada en la tabla 21.

Tabla 21: *Matriz de las vías de acción*

	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance	Web Analytics	Policy to Prevent Forum Use			Create fake postings	
Weaponization						
Delivery	NIDS, User Education	Email AV Scanning		Email Queuing	Filter but respond with out-of-office message	
Exploitation	HIDS	Patch	DEP			
Installation						
C2	NIDS	HTTP Whitelist	NIPS	HTTP Throttling		
Action on Objectives	Proxy Detection	Firewall ACL	NIPS	HTTP Throttling	Honeypot	

Fuente: Disponible en https://www.researchgate.net/figure/Kill-chain-course-of-action-matrix-developed-from-threads-1-and-2-in-Fig-4-25_fig4_330071595

Eventualmente, la organización puede hacer uso de la matriz que muestra en la tabla 20; sin embargo, lo más recomendado es adaptar la matriz a las necesidades del negocio. En este caso, es importante que la organización realice un análisis sobre los recursos que dispone para implementar diferentes mecanismos de protección en cada una de las fases. Con base a las características propias de la empresa, así como sirviéndose de la tabla anterior, se puede hacer la construcción de la matriz realizando las consideraciones necesarias.

Además, puede aprovechar las siguientes medidas generales a seguir como parte de una estrategia de implementación del marco de trabajo de Cyber Kill Chain.

- Aplicación de parches de seguridad. Aplicar parches o actualizaciones a tiempo, para el funcionamiento adecuado del sistema, con el fin de evitar problemas a nivel de funcionamiento, así como a nivel de seguridad. Estos procesos de parcheo y actualización pueden ser automatizados para un mantenimiento más eficaz.
- Programa de concientización y capacitación de los empleados. Con el fin de evitar ataques de ingeniería social, así como otros que puedan derivar de estos, la empresa debe considerar el desarrollo y mantención de un programa de concientización sobre el uso de datos de la organización por parte de sus empleados. Como parte del programa, se debe considerar la continua capacitación de los empleados, así como la aplicación de pruebas periódicas que demuestran que los empleados cumplan con el programa.
- Mantener una adecuada gestión de privilegios de acceso de los empleados. Con el fin de evitar ataques, donde se requiera el uso de privilegios administrativos u de otra índole que puedan dar acceso al atacante de instalar software malicioso; o bien, ejecutar tareas malintencionadas, debe existir una adecuada gestión de las credenciales de acceso que los empleados mantienen.
    - Implementar un sistema de correo electrónico seguro. En caso del uso de correo electrónico, el sistema deberá de contar un alto nivel de filtrado y escaneo de los correos que se reciben, incluso, que la herramienta tenga la capacidad de detectar y reportar los correos de phishing de forma inmediata e intuitiva para el usuario o empleado.
    - Utilizar solo las conexiones a internet necesarias. La organización deberá de asegurarse de utilizar las conexiones a internet que solo sean requeridas para el cumplimiento de las tareas diarias y no mantener conexiones abiertas que no se estén utilizando. Además, deberá utilizar solo estas conexiones en las horas que realmente se utilizan. Para esto, se requiere monitorizar la red y de mantener una correcta configuración de red.
    - Mantener una lista de acceso de la red. Dado que muchas de las amenazas persistentes avanzadas se sirven del acceso remoto a diferentes sistemas y crear persistencia con el fin de mantener una conexión remota, la organización deberá de mantener una lista de control de acceso para

autorizar solo a aquellos equipos o usuarios que deban de tener acceso a la red de la organización. Normalmente, estas listas de acceso se pueden definir en la configuración del firewall de la organización.

- Contrarrestar el acceso a sitios web. Debe de existir un control de acceso a los diferentes sitios web, ya sean los mismos de la organización, o bien, sitios web externos. En el caso de los sitios web de la organización, estos son específicos para el cumplimiento de deberes de los empleados; sin embargo, no todos los empleados deben tener acceso a todos los sitios web de la organización, por lo cual es importante que se limite su uso a las tareas cotidianas de los empleados. En cuanto a los sitios web externos, existen muchos sitios web maliciosos, a los cuales cualquier persona dentro de la organización podría acceder, por lo tanto, se debe restringir el uso de sitios web externos a través de administración de acceso de los equipos de los empleados y solo autorizar aquellos que sean de interés para la organización en cuanto al cumplimiento de las funciones de cada uno de los empleados.
- Mantener profesional de seguridad. La organización debe mantener un equipo especializado en ciberseguridad, el cual se encuentre completamente dedicado a las funciones de seguridad de la información de la organización. Por lo tanto, es importante considerar que este personal se encuentre capacitado y certificado para la realización de sus labores diarias, y además que no ejecuten tareas que no sean de su competencia. Dependiendo de la organización, se puede optar por contratar directamente este tipo de personal o bien adquirir un servicio tercerizado de personal de seguridad ofrecido por una empresa especializada en el tema.
- Resguardar la información fuera de la organización. Dado que actualmente se ha extendido mucho el trabajo remoto, es necesario contar con los mecanismos necesarios para resguardar la información del personal de la empresa fuera de las instalaciones del trabajo. También se considera el hecho de que hay empleados que tienen que realizar viajes o giras internacionales, donde normalmente, si se cuenta con equipo tecnológico, muchos querrán hacer una revisión exhaustiva sobre la información que se lleva consigo. Para este caso, los equipos del personal de la organización

solo deben mantener la información básica necesario para la realización de sus labores diarias y que además esta información se encuentre encriptada con algún mecanismo de encriptación seguro.

- Utilizar el factor de doble autenticación en las credenciales. Es conocido que el uso de credenciales para acceder a diferentes servicios y sistemas son tareas que frecuentemente se ejecutan por parte del personal de la empresa, estos buscan maneras más sencillas de acceder a estos, pero a su vez el uso de solo un usuario y una contraseña no basta para asegurar la información a la cual se accede. Por lo tanto, debe ser un requisito mandatorio el uso de dos factores de autenticación que coadyuven a mantener resguarda la información a la que accede dicho personal dado que si ocurre un ataque APT, una de las cosas que normalmente aprovechan estos ataques son las credenciales de los usuarios existentes o registrados en los sistemas, si los usuarios no cuentan con un factor de doble autenticación, se podrá acceder fácilmente a la información solamente conociendo el usuario y la contraseña de cada empleado.
- Restringir el acceso de los servidores a otros servidores que no sean de la organización. Uno de los objetivos principales de los atacantes es obtener acceso a los servidores de la organización; o bien, interconectar diferentes servicios a los mismos servidores con el fin de llevar a cabo un ataque en específico. Para esto, es importante el uso de firewalls con reglas de acceso bien definidas. Además, es importante evitar que los administradores de los sistemas verifiquen el correo electrónico y accedan a sitios web desde los servidores utilizando cuentas administrativas. Aplicando las medidas correspondientes, se evita que los atacantes, caso de lograr acceso a los servidores y de utilizar las cuentas administrativas de los administradores para instalar y ejecutar malware. Además, en caso de que el atacante haya logrado su objetivo, si se mantiene la correcta configuración de las cuentas administrativas, el atacante no podrá tener comunicación con el malware instalado en caso de que este se haya logrado instalar de laguna manera.
- Monitoreo del acceso remoto. Puede que el atacante se sirva de las credenciales auténticas de los empleados internos de la organización para lograr acceder a los diferentes sistemas, en dado caso, puede que no se

conozca bien que quién está conectado a la red interna de la organización no sea un empelado de la misma, o bien, que sea un exempleado que la organización mantuvo sus credenciales y logra obtener acceso. En este caso, se debería de contar con mecanismos que permitan correlacionar la información geográfica de quien está accediendo para corroborar que quién está accediendo sea un empleado auténtico de la organización y no alguien que realmente no esté autorizado. Se puede hacer uso de herramientas de correlación de eventos como un SIEM, en donde se obtenga la información precisa de los accesos y hacer investigación o análisis de inteligencia con la información suministrada para detectar algún evento sospechoso.

- Evitar el acceso remoto por parte de los administradores. Dada la importancia que tienen los servidores de dominio por el tipo de información que almacenan, como lo son las credenciales de los empleados de la organización, se debe evitar el acceso remoto a este. Ya sea dentro o fuera de la red corporativa, los atacantes no tendrían la capacidad de acceder de forma remota al servidor del controlador de dominio, aun si estos logran utilizar un equipo interno de la organización.
- Utilizar dispositivos no conectados para le resguardo de la información sensible. La organización debería almacenar información delicada, sensible o confidencial en dispositivos o equipos que no se conecten del todo a la red con el fin de evitar el acceso a dicha información, la cual solo sería accesible directamente desde el dispositivo, o bien, si se desea la extracción de esta información se puede obtener por medios físicos.
- Mantener retenida la información. Es importante que la empresa mantenga el registro sobre todos los eventos que ocurren sobre los diferentes sistemas de la organización para lograr dar trazabilidad sobre aquellos eventos que se consideren sospechosos, o en caso de que realmente se llegue a dar un ataque que se llevó a cabo y comprometió la información de la organización, con el fin de llevar a cabo un proceso investigativo en caso de ser necesario. Esto es muy importante para los ataques APT dado que por su alta sofisticación es difícil obtener datos con precisión sobre lo sucedido en el momento en el que ocurren. Esta información debería ser retenida al menos por 6 meses como mínimo.

Caso de Uso

Para demostrar el funcionamiento y aplicabilidad de la solución desarrolladas, se procede a aplicar un caso de uso, donde se siguen las diferentes etapas planteadas y eventualmente también se hace uso del instrumento de evaluación de la aplicabilidad de Cyber Kill Chain. Obsérvese las tablas 22, 23, 24, 25, 26, 27, 28 y 29, así como las figuras 29, 30, 31, 32, 33, 34, 35 y 36.

Tabla 22: *Etapa de reconocimiento*

ID	Activo	Cantidad	Tipo/Descripción
1	Computadoras	20	Hardware
2	Servidor de archivos	2	Hardware
3	Servidor de correo	2	Hardware
4	Servidor FTP	2	Hardware
5	Servidor Web	2	Hardware
6	Servidor NTP	2	Hardware
7	Servidor Bases de Datos	2	Hardware
8	Servidor de aplicaciones	2	Hardware
9	Servidor de controlador de dominio	1	Hardware
10	Aplicaciones empresariales	10	Software
11	Enrutadores	3	Hardware
12	Switches	4	Hardware
13	Puntos de Acceso	4	Hardware
14	Dispositivo NAS	2	Hardware

Fuente: Elaboración propia.

Tabla 23: *Etapa de diagnóstico*

ID	Controles	Tipo/Descripción
1	Políticas de gestión de comunicaciones	Governanza
2	Políticas de gestión de acceso a activos de información y datos	Governanza
	Políticas de respaldo y almacenamiento de la información	Governanza
3	Administración de permisos y privilegios	Governanza

ID	Controles	Tipo/Descripción
4	Múltiple Factor de Autenticación	Tecnología
5	Registro y trazabilidad sobre eventos de los equipos	Tecnología
6	Herramientas para bloqueo de ataques de denegación de servicio (DDoS)	Tecnología
7	Análisis del tráfico de red	Tecnología
8	Sistemas de detección y prevención de intrusos	Tecnología

Fuente: Elaboración propia.

Tabla 24: *Etapa de análisis*

ID	Categoría	Vulnerabilidades y Amenazas
1	Ingeniería Social	Dumpster diving
		Shoulder surfing
		Phishing
		Spam
		Pérdida y robo de activos de información y datos
		Pharming
2	Software	Adware
		Exploits
		Malware
		Spyware
3	Autenticación	Spoofing-Looping
		IP Splicing-Hijacking
		Spoofing
		Net Flooding
4	Monitorización	Scanning
		Snooping-Downloading
		TCP Connect Scanning
		TCP SYN Scanning
		Tampering / Data Diddling

ID	Categoría	Vulnerabilidades y Amenazas
5	Modificación, alteración o destrucción	Borrado de Huellas
		Software weakness

Fuente: Elaboración propia.

Etapa de implementación

Aplicación del instrumento de evaluación de aplicabilidad de Cyber Kill Chain.

Tabla 25: *Etapa de análisis*

Análisis Nivel de Implementación Cyber Kill Chain			
Etapas y Fases	Preguntas	Respuestas	
Etapa de pre compromiso		Sí	No
Reconocimiento	¿Existen mecanismos para la protección de información pública de la organización que pueda revelar datos confidenciales?		x
	¿Existen mecanismos para el control de perfiles completos sobre la organización en la		x
	¿Existe información confidencial expuesta al público?	x	
	¿La información de los sistemas que componen la infraestructura de TI de la organización es díficil de obtener?		x
	¿Existen mecanismos de control para la protección de los nombres de dominio?	x	
	¿Los sitios web de la empresa implementan mecanismos de seguridad?	x	
	¿Los puertos de los diferentes servidores y sistemas están protegidos?		x
	¿Existen mecanismos control de anti spam?		x
	¿La organización implementa políticas para mitigar o evitar el phishing?		x
	¿La organización implementa controles de seguridad orientados a la ingeniería social?		x
	¿La organización implementa mecanismos de analítica web?	x	
	¿La organización implementa políticas orientadas a la regulación de la información que se publica en la web?	x	
	¿La organización implementa firewalls en su infraestructura?	x	
	¿La organización implementa sistemas de prevención intrusiones?	x	
	¿La organización implementa mecanismos de autenticación?	x	
	¿Existen políticas de control sobre el uso de las redes sociales?		x
	¿En caso de publicarse información que debe mantenerse pública, se aplican métodos de cifrado de la información para impedir accesos no autorizados?		x
	¿En caso de utilizar servicios públicos en la nube, la información que maneja está protegida, o bien, es información que no revela datos importantes sobre la compañía?		x
	¿La organización implementa mecanismos orientados a proteger perímetro más externo de la red?		x
	¿La organización conoce todos los puntos de entrada de los diferentes sistemas?		x

Preparación	¿La organización implementa mecanismos de control y trazabilidad de puertas traseras?	x	
	¿La organización implementa mecanismos de control y trazabilidad para el acceso remoto?	x	
Distribución	¿La organización implementa un programa de concientización sobre ingeniería social?		x
	¿La organización implementa sistemas de detección y de filtro de correos maliciosos?	x	
	¿La información de los empleados no se encuentra expuesta como para recibir información que no sea de competencia para la compañía?		x
	¿La información de identidad de los usuarios o empleados se encuentra protegida?		x
	¿Existen datos de la organización que puedan ser difícilmente enmascarados?	x	
	¿Se implementa algún mecanismo de control para evitar el enmascaramiento de datos o información de la organización?		x
	¿Existen mecanismos para contrarrestar la descarga de archivos, en cualquier formato existente, no autorizados o sospechosos?		x
	¿Existen mecanismos o medidas para la protección de los medios físicos usb?		x
	¿Se implementan mecasnimos para evitar o contrarrestar vulnerabilidades a nivel de DNS?	x	
	¿Se implementan mecanismos de captura de paquetes para el análisis de red?		x
	¿Existe un control exhaustivo sobre el tráfico de red de la organización?	x	
	¿Existen métodos para medir los niveles de implementación de los programas de concientización?		x

Etapa de compromiso			
Explotación	¿Los sistemas operativos y el software que se utiliza en la organización son seguros?		x
	¿Los sistemas operativos y el software que se utiliza en la organización son debidamente mantenidos?	x	
	¿Se implementa software anti virus en los diferentes equipos de los empleados?		x
	¿Existen mecanismos de control para el acceso remoto por medio de consola?	x	
	¿La organización cuenta con mecanismos de seguridad para exploits?	x	
	¿La organización cuenta con mecanismos de seguridad para ataques de denegación de servicios?	x	
	¿La organización cuenta con mecanismos de seguridad para la protección de explotaciones a nivel de protocolos (FTP, SMTP, NTP, SSH, entre otros)?		x
	¿La organización cuenta con mecanismos de seguridad contra ataques dirigidos a la administración de la memoria de los diferentes equipos?		x
	¿La organización cuenta con sistemas de detección de intrusos en la red?	x	
	¿Existen mecanismos para la detección de anomalías en los datos entrantes y salientes de la red de la organización?	x	
	¿La organización da un seguimiento sobre las detecciones o monitores que se realizan a nivel de los sistemas?	x	
	¿La organización hace uso de indicadores de compromiso así como de otros indicadores con el fin de mejorar el proceso de análisis en las detecciones y el monitoreo?		x
	¿La acciones de las detecciones o monitoreo que se realiza están automatizadas?		x
	¿La organización implementa mecanismos de registro de logs de los diferentes sistemas?	x	
	¿La organización implementa una política de retención de registros de logs?	x	
	¿La organización implementa mecanismos para la correlación de eventos o registros logs?	x	
Instalación	¿Existen controles de seguridad a nivel de los equipos de los usuarios que eviten la instalación ejecución de software malicioso?		x
	¿La configuración en los equipos evita que los usuarios, aplicaciones o servicios puedan ejecutar tareas sin autorización de la organización?		x
	¿Existen mecanismos de seguridad que eviten que se inicien aplicaciones o servicios de manera automática al iniciar los equipos de los usuarios o empleados?		x
	¿Existen mecanismos para el tratamiento de amenazas críticas como el ransomware?	x	
	¿Existen sistemas de respaldo que faciliten la recuperación de la información en caso de pérdida de la misma?		x
	¿Se realiza un análisis de malware en sospechas malware?	x	

Comando y control	¿Existen mecanismos de seguridad que eviten la exfiltración de la información de la organización?		x
	¿Existen mecanismos de control para evitar la comunicación de los sistemas de la organización con servidores externos maliciosos?		x
	¿Existen mecanismos para interrumpir accesos o comunicaciones remotas no permitidas?	x	
	¿Existen mecanismos para filtrar las direcciones IP y los protocolos HTTP?	x	
	¿Se implementan mecanimos de seguridad que permitan limitar las solicitudes HTTP?	x	
	¿Existen mecanismos para detectar actividad inusual en las cuentas de los usuarios?	x	
Acciones sobre objetivos	¿Los sistemas de la organización son interdependientes o se implementan mecanismos de seguridad que eviten ataques masivos sobre los distitntos sistemas de la organización?		x
	¿Existen mecanismos para evitar que los sitemas de la organización se puedan utilizar para ataques basados en botnets?		x
	¿Existen controles que eviten el control directo sobre los diferentes equipos o sistemas de la organización?		x
	¿Las credenciales de los sistemas y de los usuarios están debidamente protegidas?	x	
	¿Se implementan sistemas de seguridad que permitan la detección o revisión de proxies?	x	
	¿Se implementan firewalls basados en lista de control de acceso?		x
	¿Se implementa una infraestructura basada en honeypots?		x

Fuente: Elaboración propia.

Tabla 26: *Datos estadísticos de las fases*

Datos Estadísticos de las Fases			
Fases	Total Preguntas	Resultados Afirmativos	Resultados Negativos
Reconocimiento	20	8	12
Promedio Reconocimiento		0.4	0.6
Nivel de Implementación		2	3
Preparación	2	2	0
Promedio Preparación		1	0
Nivel de Implementación		5	0
Distribución	12	4	8
Promedio Distribución		0.33	0.67
Nivel de Implementación		1.65	3.35
Explotación	16	10	6
Promedio Explotación		0.63	0.38
Nivel de Implementación		3.15	1.9
Instalación	6	2	4
Promedio Instalación		0.33	0.67
Nivel de Implementación		1.65	3.35
Comando y control	6	4	2
Promedio Comando y control		0.67	0.33
Nivel de Implementación		3.35	1.65
Acciones sobre objetivos	7	2	5
Promedio Acciones sobre ob		0.29	0.71
Nivel de Implementación		1.45	3.55

Fuente: Elaboración propia.

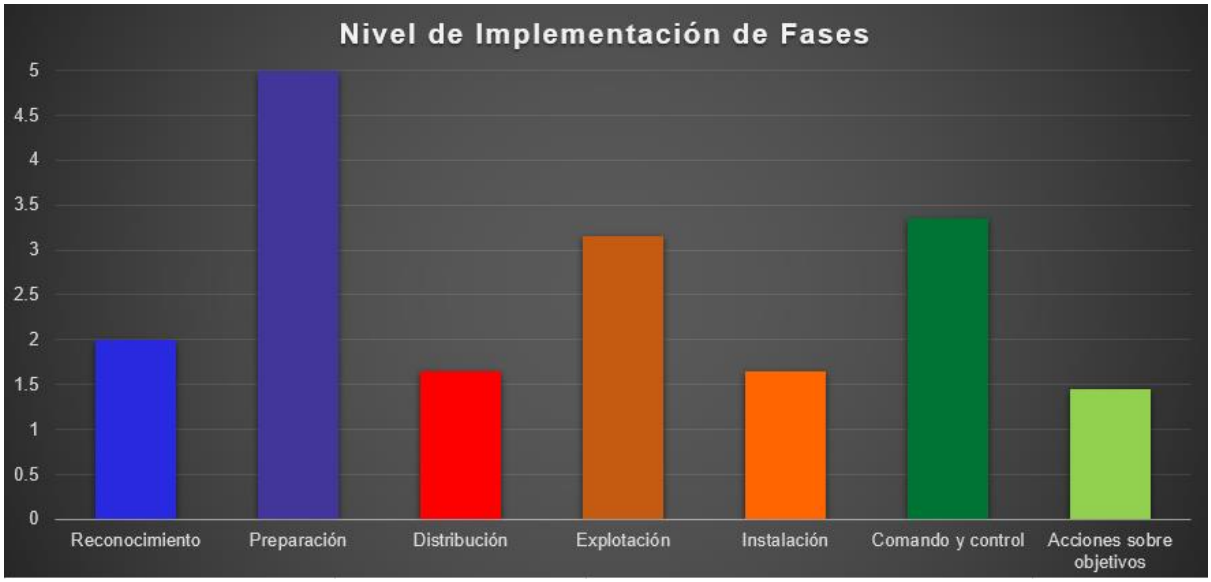


Figura 29: Nivel de implementación de fases. Fuente: Elaboración propia.

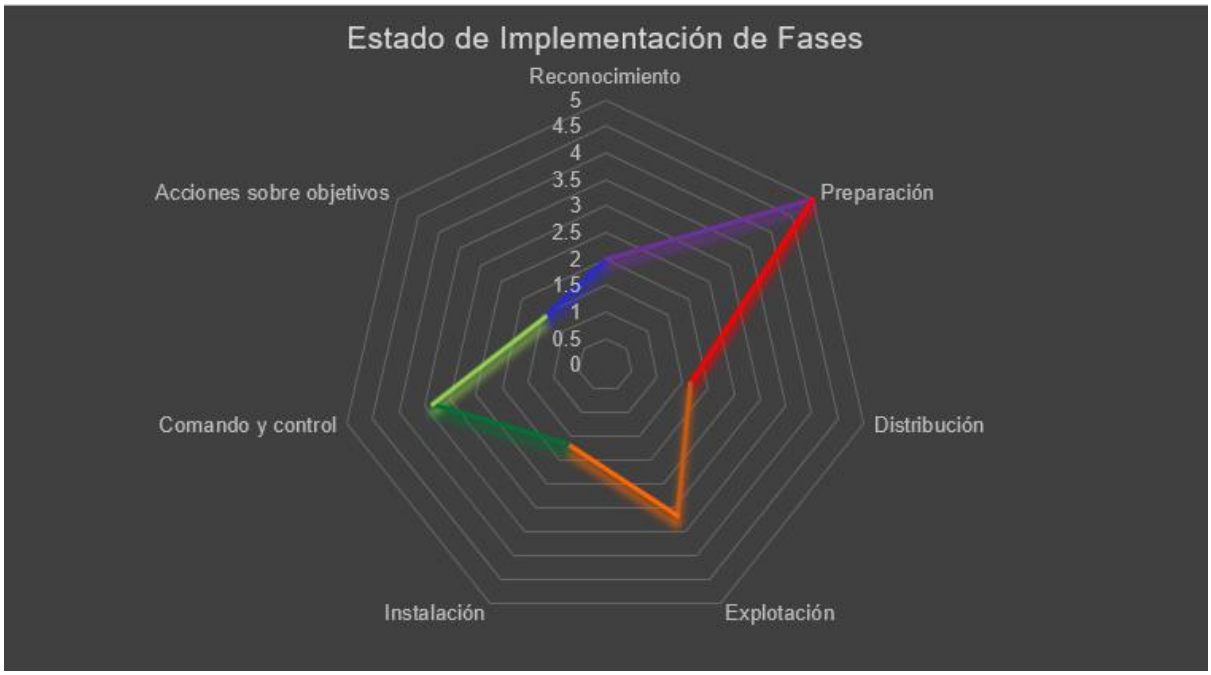


Figura 30: Estado de implementación de fases. Fuente: Elaboración propia.

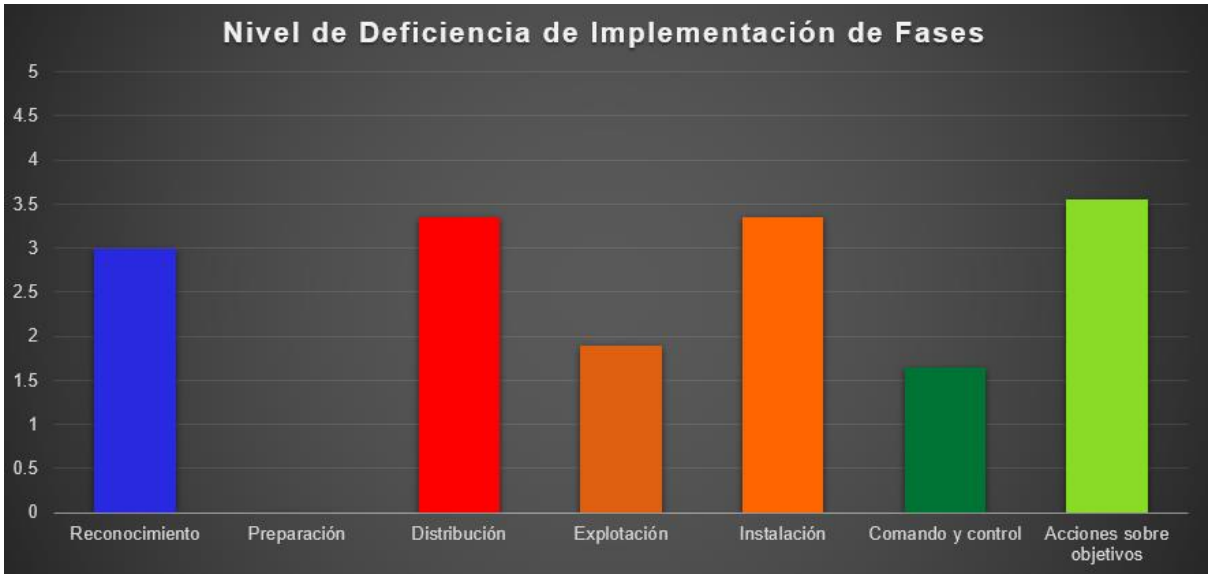


Figura 31: Nivel de deficiencia de implementación de fases. Fuente: Elaboración propia.

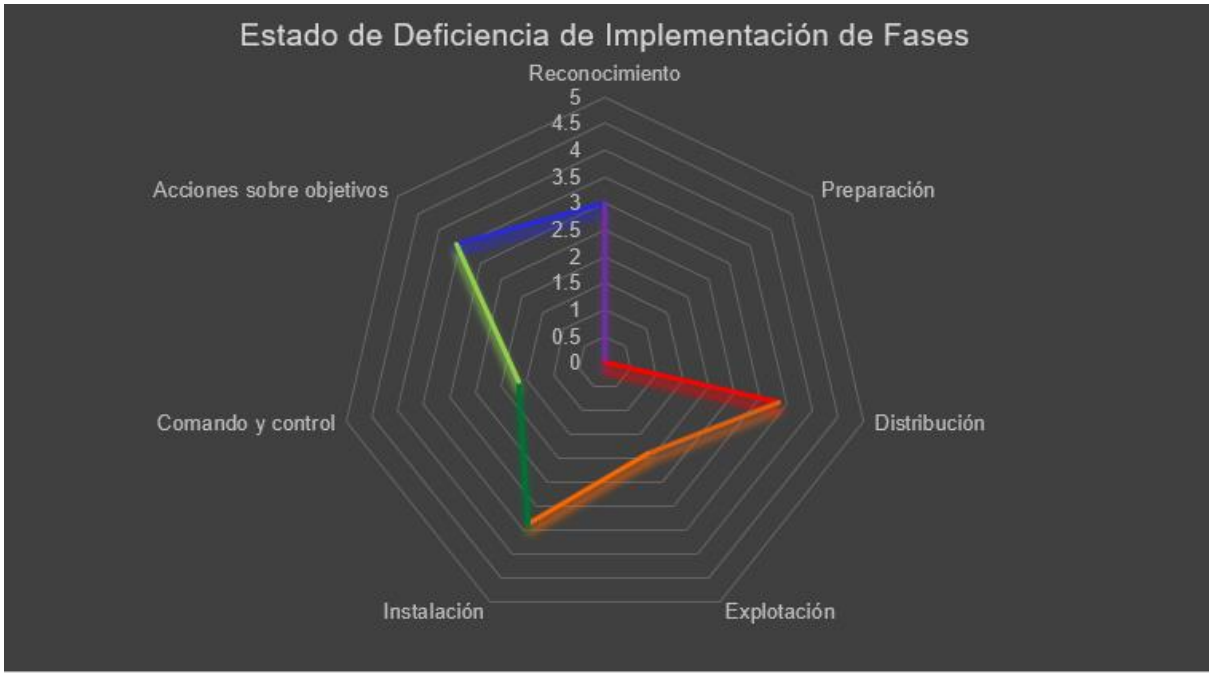


Figura 32: Estado de deficiencia de implementación de fases. Fuente: Elaboración propia.

Tabla 27: *Datos estadísticos de las etapas*

Datos Estadísticos de las Etapas			
Etapas	Total Preguntas	Resultados Afirmativos	Resultados Negativos
Pre compromiso	34	14	20
Promedio Pre Compromiso		0.41	0.59
Nivel de Implementación		2.05	2.95
Compromiso	22	12	10
Promedio Compromiso		0.55	0.45
Nivel de Implementación		2.75	2.25
Post Compromiso	13	6	7
Promedio Post Compromiso		0.46	0.54
Nivel de Implementación		2.3	2.7

Fuente: Elaboración propia.

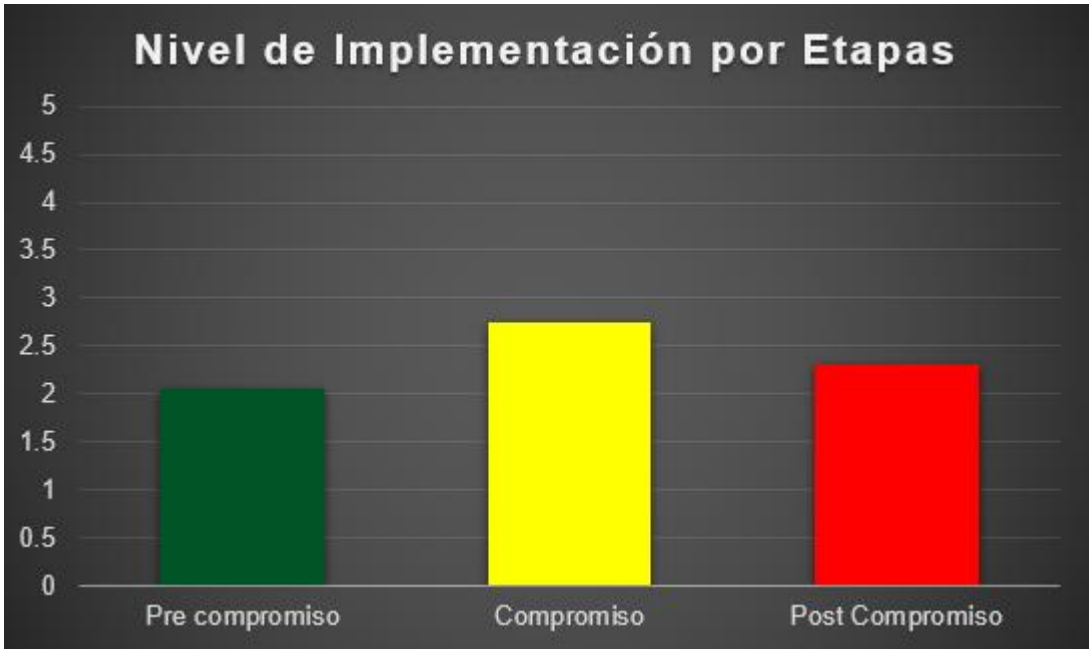


Figura 33: Nivel de implementación por etapas. Fuente: Elaboración propia.

Figura 34: Estado de implementación por etapas. Fuente: Elaboración propia.

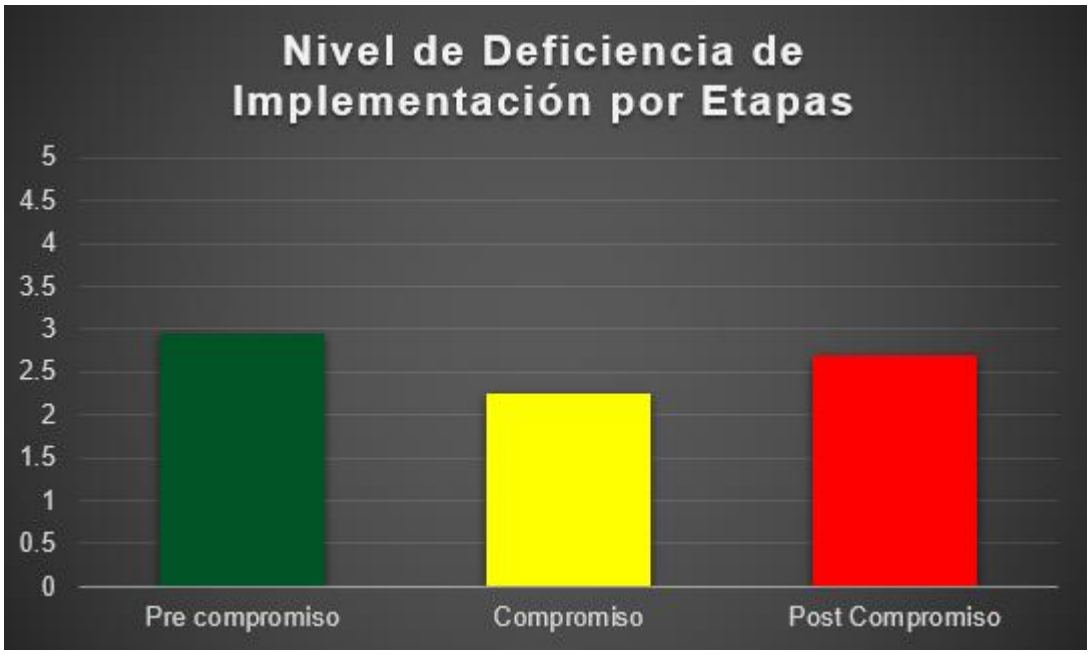


Figura 35: Nivel de deficiencia de implementación por etapas. Fuente: Elaboración propia.

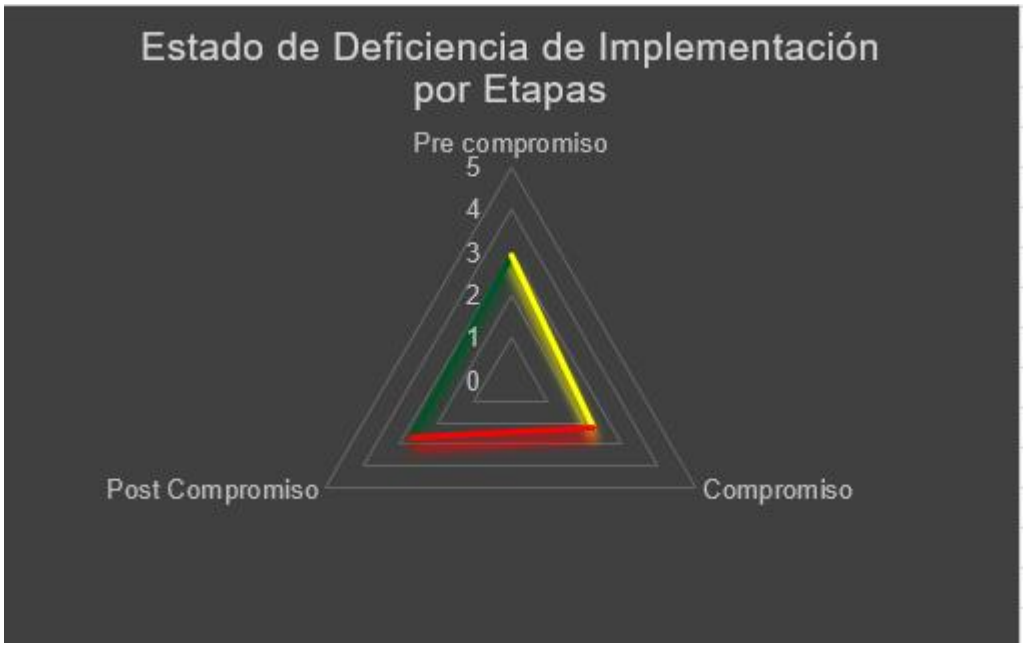


Figura 36: Estado de deficiencia de implementación por etapas. Fuente: Elaboración propia.

Tabla 28: *Nivel de implementación Cyber Kill Chain*

Nivel de Implementación Cyber Kill Chain		
0	Inexistente	La fase o la etapa no se ha aplicado y no existe ninguna estrategia relacionada que se haya aplicado
1	Inicial	La fase o la etapa ha sido considerada por la organización por lo que se encuentra en un etapa inicial, sin embargo, no se ha comenzado a desarrollar
2	En proceso	La fase o la etapa se encuentra en un proceso de desarrollo
3	Implementado	La fase o la etapa se ha logrado implementar, sin embargo, no se ha desarrollado y no ha a alcanzado un nivel de madurez alto
4	Avanzado	La fase o la etapa ha logrado alcanzar cierto nivel de madurez con respecto a su implementación, sin embargo, no ha alcanzado su nivel máximo
5	Completado	La fase ola etapa se ha logrado implementar en su completitud

Fuente: Elaboración propia.

Tabla 29: *Nivel de implementación Cyber Kill Chain*

Análisis Nivel de Implementación Cyber Kill Chain		
Etapas y Fases	Nivel de Implementación Positivo	Nivel de Implementación Negativo
Etapa de pre compromiso	2.05	2.95
Reconocimiento	2	3
Preparación	5	0
Distribución	1.65	3.35
Etapa de compromiso	2.75	2.25
Explotación	3.15	1.9
Instalación	1.65	3.35
Etapa de post compromiso	2.3	2.7
Comando y control	3.35	1.65
Acciones sobre objetivos	1.45	3.55

Fuente: Elaboración propia.

Etapa de resultados

Según los resultados obtenidos, la etapa de pre-compromiso muestra estar en un nivel de implementación de 2.05, por lo cual se identifica como en un estado en proceso de implementación; sin embargo, el nivel de implementación negativo es de 2.95, lo cual demuestra que el estado general no es bueno. Considerándose las fases de esta etapa, las fases de reconocimiento y distribución mostraron ser las más graves, dado que muestran bajos niveles de implementación. En el caso de la fase de reconocimiento se encuentra en proceso de implementación y la fase de distribución se encuentra en un estado inicial de implementación. Además, la fase de preparación es la que se en encuentra completamente implementada.

Considerándose estos datos, la organización debe de mejorar la implementación de Cyber Kill Chain y mejorar la etapa pre-compromiso orientándose, principalmente, a mejorar las fases de reconocimiento y de distribución según una cadena de ataque.

La etapa de compromiso muestra estar en un nivel de implementación de 2.75, por lo cual se identifica como en un estado en proceso de implementación; sin embargo, el nivel de implementación negativo es de 2.25, lo cual demuestra que el estado general está bien, pero se debería mejorar. Considerándose las fases de esta etapa, la fase de explotación es la que se encuentra en un estado intermedio de implementación, por lo cual se considera como implementado, mientras que la fase

de instalación muestra un estado inicial, es decir, se está comenzando a implementar, el cual es muy bajo. Considerándose la etapa, así como sus respectivas fases, la organización debe de mejorar la implementación del marco de trabajo de Cyber Kill Chain con respecto a la etapa de pre-compromiso, donde debe realizar mayores esfuerzos por mejorar la fase de instalación y continuar optimizando la implementación en la fase de explotación.

Concluyendo, los resultados obtenidos del instrumento de evaluación, la etapa de post compromiso muestra un nivel de implementación de 2.3, por lo cual se identifica como en un estado en proceso de implementación; sin embargo, el nivel de implementación negativo es de 2.7, lo cual demuestra que se debe de mejorar esta etapa. Considerándose las fases de esta etapa, la fase de comando y control es la que se encuentra en un estado intermedio de implementación, por lo cual se considera como implementado, mientras que la fase de acciones sobre objetivos muestra un estado inicial, se está comenzando a implementar. Por lo tanto, considerándose la etapa, así como sus respectivas fases, la organización debe de mejorar la implementación del marco de trabajo de Cyber Kill Chain con respecto a la etapa de post compromiso en donde debe realizar mayores esfuerzos por mejorar la fase de acciones sobre objetivos y continuar optimizando la implementación en la fase de comando y control.

Capítulo 6. Conclusiones y Recomendaciones

6.1 Conclusiones

Conclusiones del objetivo 1: “Identificar las estrategias de seguridad de la información que se hayan implementado en el país por medio del estudio de las diferentes leyes, políticas y estándares del país, para identificar áreas de mejora”.
Se concluye:

- Como parte del logro de este objetivo, se requirió la realización de consulta e investigación sobre diferentes fuentes de información, principalmente de medios de comunicación masivos, noticias, entrevistas, documentos empresariales y documentos legales, donde se realizó un proceso de trazabilidad de la información para corroborar cuáles aspectos estuvieron relacionados a áreas u oportunidades de mejora.

- Es importante que a pesar de que la mayoría de los medios de los cuales se obtuvo la información necesaria para el cumplimiento de este objetivo eran relevantes, se logró detectar que los medios noticiosos ofrecían mayor detalle sobre la información que se requería y ofrecían diferentes perspectivas o puntos de vista, los cuales fueron de gran ayuda para obtener un criterio más objetivo y claro sobre la realidad que sucede en el país.
- Los medios de comunicación también ofrecieron información a partir de entrevistas que se realizaron a profesionales en el campo de la seguridad de la información, los cuales eran nacionales, esto también sirvió para enriquecer la información y así fundamentar más la investigación.

Conclusiones del objetivo 2: “Comprender las estrategias implementadas en el país a través del análisis de la información obtenida, para definir el contexto sobre el cual se analizará el marco de trabajo”.

Se concluye:

- Para el cumplimiento de este objetivo, dado que se debía de realizar la recopilación de la información, para luego identificar falencias relacionadas al estado de la seguridad de la información en el país, se tuvo que realizar un exhaustivo proceso de análisis sobre esta información para identificar las estrategias de seguridad de la información que se hayan implementado en el país.
- Como parte del proceso de análisis se consideró también la documentación elegida en la investigación con la cual se estableció un contexto aun más amplio de información sobre el marco de trabajo de Cyber Kill Chain.
- Un ejemplo de cómo se logró obtener más información de contexto fue que una vez que se corroboró que el país había sido afectado por amenazas persistentes avanzadas y que con la información que se obtuvo con el primer objetivo se detectó que no existían los elementos o mecanismos necesarios para la protección de este tipo de ataques, se procedió a investigar a mayor profundidad este tipo de amenazas. Con el estudio de las amenazas persistentes avanzadas también se detectó el gran vinculo existente con el marco de trabajo de Cyber Kill Chain como solución para estas mismas.
- Cabe señalar que también se detectaron otros modelos, soluciones y marcos de trabajo orientados a mitigar las amenazas persistentes avanzadas; sin

embargo, luego de un proceso de análisis se estableció continuar trabajando con el marco de trabajo de Cyber Kill Chain dado que ha demostrado ser muy eficaz para esta problemática.

Conclusiones del objetivo 3: “Desarrollar un proceso de investigación a través de la recolección de información por medio una encuesta, para obtener información más precisa sobre el uso y la aplicabilidad del marco de trabajo de Cyber Kill Chain”.
Se concluye:

- Dado que era necesario obtener información más exacta sobre el marco de trabajo de Cyber Kill Chain, con base al cumplimiento del objetivo anterior, se aplicó una encuesta a diferentes participantes la cual reveló información de gran importancia, dado que esta procedía de profesionales relacionados al área de la informática.
- Se logró obtener más información de contexto, que aunada a la que se obtuvo a partir de los otros dos objetivos anteriores, se establecieron las bases principales del desarrollo de la solución planteada en esta investigación. En otras palabras, es con el cumplimiento de este objetivo que se logra establecer las bases fundamentales de la investigación.
- Lo que más destacó en el logro de este objetivo, es que dado que se requería conocer el estado de la seguridad de la información con respecto al uso y la aplicación del marco de trabajo de Cyber Kill Chain; este reveló que la mayoría de los participantes lo desconocían. Es un dato curioso dado que este marco de trabajo tiene bastante tiempo de existir y también es conocido que hay empresas que, si lo implementan, pero son muy pocas las que lo hacen o tan si quiera lo conocen.

Conclusiones del objetivo 4: Analizar el marco de trabajo de Cyber Kill Chain a través del estudio de su estudio, para definir su aplicabilidad en el contexto del país.
Se concluye:

- Para el cumplimiento de este objetivo, se realizó un estudio y un análisis profundo sobre el marco de trabajo de Cyber Kill Chain y sobre las amenazas persistentes avanzadas. Con esta información se terminó de validar la efectividad del marco de trabajo de Cyber Kill Chain para este tipo de amenazas.

- Considerando las bases de la investigación, se relacionó la gran vulnerabilidad que tiene el país frente a las amenazas persistentes avanzadas, por lo cual a partir de esto y a partir de la efectividad comprobada de Cyber Kill Chain sobre las APTs, se consideró y corroboró que este marco de trabajo se ajustaba muy bien para cubrir las necesidades del país. Esto quiere decir, que la aplicabilidad de este marco de trabajo se ajusta a lo que busca este objetivo, el cual es su aplicabilidad considerando el contexto de la problemática de las amenazas persitentes avanzadas en el país.
- Se identificó que el marco de trabajo de Cyber Kill Chain es muy dinámico, en el sentido de que perfectamente puede ser ajustado e implementado por cualquier organización en el país.

Conclusión del objetivo general: “Proponer un instrumento de evaluación de la aplicabilidad del marco de trabajo Cyber Kill Chain, para el establecimiento de estrategias de seguridad de la información en las organizaciones en Costa Rica”.

- Para el cumplimiento de este objetivo, se desarrolló el instrumento de evaluación de la aplicabilidad del marco de trabajo de Cyber Kill Chain, con el cual ahora las organizaciones, sin importar su tamaño, pueden hacer uso de esta herramienta para evaluar si es necesario o no aplicarlo. El funcionamiento de este se basa en una serie de pasos a seguir para llevar a cabo dicha evaluación sobre la cual estará a cargo un profesional relacionado al área de seguridad de la información en la organización por lo que, además; el analista, el encargado o el estratega a cargo tendrá un criterio más claro y profundo para tomar una decisión estratégica en su organización.

Además de las ventajas anteriormente mencionadas, se destaca que este instrumento también sirve:

- Como una guía para conocer el estado de seguridad de la información de la organización.
- Como generador de conciencia en todas las personas involucradas en diferentes procesos del negocio en relación con las potenciales amenazas que puedan afectar a la organización.
- Para promover el uso e implementación de estándares y políticas orientadas a mejorar el estado de la seguridad de la información.

Como parte de la solución, se generaron una serie de recomendaciones estándar que un profesional puede considerar en caso de que proceda a la implementación del marco de trabajo de Cyber Kill Chain y, además, con el fin de comprobar la efectividad del uso de esta herramienta, se aplicó un caso de uso en donde se demuestra cómo utilizarlo y los resultados que genera después de su aplicación. Este caso de uso también sirve como una guía al profesional encargado de aplicar la evaluación, porque cuenta con un modelo o ejemplo a seguir para la aplicación de este instrumento.

6.2 Recomendaciones

A continuación, se presentan algunas recomendaciones basadas en la experiencia del desarrollo del presente trabajo de investigación, considerando diferentes aspectos tales como estándares, uso del tiempo y costo financiero.

- Con el fin de mejorar la calidad de un trabajo de investigación, si el investigador cuenta con los recursos financieros necesarios para obtener otras fuentes de información, es recomendable que invierta en obtener aquellas fuentes que solo se puedan obtener a través del pago de rstas. Esto a razón de que entre mejor sea la cantidad de fuentes consultadas más calidad tendrá el trabajo. Además, las versiones de pago de muchos documentos de investigación normalmente son más completos que su versión gratuita, o bien, muchos documentos gratuitos no contienen la información que se requiere para mejorar la calidad de la investigación.
- Es recomendable, en la medida de lo posible, consultar la mayor cantidad de expertos relacionados al tema de investigación. Esto porque si se realizan las consultas a pocos expertos, baja el nivel de objetividad sobre la información obtenida de estos. Esto quiere decir que, si se realizan más consultas a diferentes expertos, se va a obtener mayor objetividad en la información y de esta manera lograr un criterio más acertado al momento de desarrollar la investigación.
- En relación con el tiempo y la ejecución de tareas, es importante el tema de la organización. Esto quiere decir que, la calidad de un trabajo de investigación

también puede mejorar o mantener un estándar de calidad si el investigador define y gestiona tareas según el tiempo del que disponga para su desarrollo.

- Considerando aspectos técnicos o específicos de la investigación, en este caso se desarrolló un instrumento de evaluación para un marco de trabajo específico; sin embargo, podrían desarrollarse más bajo la misma premisa, o bien considerando otros marcos de trabajo que posiblemente no se hayan considerado por razones distintas.
- En cuanto a la creación del instrumento de evaluación, es recomendable definir reglas claras y específicas sobre su uso, dado que es muy importante que quien vaya a hacer uso de este no tenga que estar recurriendo a otras fuentes, solamente para corroborar la misma información, o bien para saber cómo aplicar el proceso. Por esta misma razón, en este trabajo también se aplica un caso de uso del instrumento.
- En cuanto a los cálculos realizados para la generación de valores cuantitativos utilizados en el instrumento, es recomendable especificar cómo se calcula cada valor y el significado que tiene cada uno. Por lo que los datos cuantitativos deben expresarse también de manera cualitativa, con el fin de que la persona encargada de utilizar dicho instrumento descifre con mayor precisión los datos, con el fin de evitar ambigüedades o malas interpretaciones.

Capítulo 7. Reflexiones Finales

Este proyecto se estableció a partir de la inquietud del autor por investigar más sobre el tema de las amenazas persistentes avanzadas, así como el tema de Cyber Kill Chain, los cuales luego de haberse desarrollado el trabajo de investigación han demostrado ser muy interesantes, no solo por lo que representan en el ámbito de la seguridad de la información, sino también por el impacto que tienen en la sociedad. Cada vez se observa con más frecuencia como las organizaciones, tanto en Costa Rica como en el mundo, son afectadas por las amenazas persistentes avanzadas, lo cual ha demostrado ser un tema de interés no solo por expertos relacionados al campo de la seguridad de la información, sino que también es de interés para todo el mundo, pues su impacto es general a pesar de que se tiende a pensar que solamente impacta a las organizaciones que son afectas. Además, conforme avanza la

tecnología y las soluciones de ciberseguridad, así también avanzan este tipo de amenazas, las cuales no dejan de evolucionar y se van volviendo más complejas con el paso del tiempo, razón por la cual se deben de generar o aplicar medidas que las contrarresten, por lo que se consideró el marco de trabajo de Cyber Kill Chain, el cual ha demostrado ser eficaz para este tipo de amenazas y a la vez se puede acoplar a la mayoría de las organizaciones que deseen mejorar el estado de seguridad de la información.

Otro de los intereses que tuvo el autor para desarrollar este trabajo de investigación, es que notó la necesidad de generar conciencia sobre las amenazas persistentes avanzadas, así como sobre otras amenazas existentes en temas de ciberseguridad y la preocupación de continuar avanzado en el desarrollo de la ciberseguridad en Costa Rica. Es conocido que estas amenazas afectan a muchos países; sin embargo, Costa Rica ha considerado mejorar el estado de seguridad de la información por medio del desarrollo de diferentes políticas legislativas, así como el desarrollo de diferentes programas y planes orientados a mitigar el impacto de las amenazas cibernéticas. Sin embargo, no escapa de la realidad: es complejo tratar las amenazas persistentes avanzadas, por lo cual es requerido continuar haciendo esfuerzos en este ámbito de la ciberseguridad.

Capítulo 8. Trabajos a Futuro

A continuación, se establecen los posibles trabajos a futuro que se podrían desarrollar a partir de la presente investigación:

- Oportunidad de ampliación del instrumento. El presente instrumento se puede seguir desarrollando, considerando que se podría ampliar o desarrollar otros cuestionarios que mantengan estrecha relación con las evaluaciones establecidas. Además, con esto, se podrían desarrollar más cálculos para la generación de nuevas estadísticas que ofrezcan mayor detalle de criterio a los profesionales que vayan a hacer uso de ella.
- Desarrollar otros modelos de evaluación de la aplicabilidad. Con base a la estructura del instrumento generado, se pueden generar otros instrumentos para otros marcos de trabajo que no se consideraron dentro del alcance del presente trabajo de investigación.
- Se podría desarrollar otros modelos de evaluación o de madurez orientados al tratamiento de las amenazas persistentes avanzadas de una forma más global, en el sentido que estas mismas evolucionarán con el tiempo, por lo que se podrían considerar temas como big data, inteligencia artificial, computación en la nube o de cualquier otra índole que no se haya considerado en la presente investigación.

Glosario

A

Amenaza de nueva generación. Ataque cibernético que tiene la capacidad de propagarse fácilmente a través de cualquier medio sin importar la arquitectura, los equipos. (Tounsi, Wiem & Rais, Helmi. (2017)).

B

Amenaza persistente avanzada (APT). Ciberataque dirigido y muy sofisticado. (Quintero-Bonilla, S., & Martín del Rey, A. (2020)).

C

Amenazas polimórficas. Amenaza que tienen la capacidad de evolucionar o cambiar su comportamiento durante la ejecución de un ataque (virus, gusanos o troyanos que cambian constantemente). (Tounsi, Wiem & Rais, Helmi. (2017)).

D

Ataque de día cero. Acometida que aprovecha vulnerabilidades en software o sistema, al cual no se le ha desarrollado o aplicado una solución para atender su vulnerabilidad. (Bahrami, P. N., Dehghantanha, A., Dargahi, T., Parizi, R. M., Choo, K. K. R., & Javadi, H. H. (2019)).

E

Cyber Kill Chain. Marco de trabajo de seguridad. Busca comprender cómo funciona un ataque para enriquecer la comprensión de las tácticas, técnicas y procedimientos utilizados por los atacantes. (Quintero-Bonilla, S., & Martín del Rey, A. (2020)).

F

Grupos APT. Ejecutores de las amenazas persistentes avanzadas. (Bahrami, P. N., Dehghantanha, A., Dargahi, T., Parizi, R. M., Choo, K. K. R., & Javadi, H. H. (2019)).

Referencias

Bahrami, P. N., Dehghantanha, A., Dargahi, T., Parizi, R. M., Choo, K. K. R., & Javadi, H. H. (2019). Cyber kill chain-based taxonomy of advanced persistent threat actors: analogy of tactics, techniques, and procedures. *Journal of Information Processing Systems*, 15(4), 865-889. Obtenido de: http://jips-k.org/digital-library/2019/15/4/865: http://jips-k.org/journals/jips/digital-library/manuscript/file/23042/JIPS-2019-15-4-865.pdf

Quintero-Bonilla, S., & Martín del Rey, A. (2020). A New Proposal on the Advanced Persistent Threat: A Survey. *Applied Sciences*, *10*(11), 3874. Obtenido de https://www.researchgate.net/publication/341904556_A_New_Proposal_on_the_Advanced_Persistent_Threat_A_Survey: https://www.researchgate.net/publication/341904556_A_New_Proposal_on_the_Advanced_Persistent_Threat_A_Survey/fulltext/5ee046a7a6fdcc4768943a88/A-New-Proposal-on-the-Advanced-Persistent-Threat-A-Survey.pdf

Saborío, Paulo Villalobos. “Costa Rica Fue Blanco De Ataques De Espionaje Cibernético De Corea Del Norte En 2018, Según Informe.” ameliarueda.com. AmeliaRueda.com, April 6, 2019. https://www.ameliarueda.com/nota/costa-rica-blanco-ataques-espionaje-cibernetico-corea-norte-informe.

Vinculan hackers de Corea del Norte con ola de ciberataques a bancos en todo el mundo. (2018, October 03). Retrieved June 25, 2021, from https://www.monumental.co.cr/2018/10/03/vinculan-hackers-de-corea-del-norte-con-ola-de-ciberataques-bancos-en-todo-el-mundo/

Costa Rica recibió 19 millones de ciberataques durante primer trimestre: Sector público no está preparado. (n.d.). Retrieved June 25, 2021, from https://www.crhoy.com/tecnologia/costa-rica-recibio-19-millones-de-ciberataques-este-semestre-sector-publico-no-esta-preparado/

Sampieri, R., Collado, C. & Lucio, P. (2014). *Metodología de la investigación*. México, D.F: McGraw-Hill Education.

Tatam, M., Shanmugam, B., Azam, S., & Kannoorpatti, K. (2021). A review of threat modelling approaches for APT-style attacks. *Heliyon*, *7*(1). Obtenido de: https://www.sciencedirect.com/science/article/pii/S2405844021000748: https://reader.elsevier.com/reader/sd/pii/S2405844021000748?token=33AA4EBEE6E4A6D49EAB8DF74ACB2AC9A25F88F92D8FEAC4C28028A44E29AF1087071C862A08F4EDDB8B60824CFF3738&originRegion=us-east-1&originCreation=20210429235049

Tounsi, W., & Rais, H. (2018). A survey on technical threat intelligence in the age of sophisticated cyber attacks. Computers & Security, 72, 212–233. Obtenido de: https://www.researchgate.net/publication/320027747_A_survey_on_technical_threat_intelligence_in_the_age_of_sophisticated_cyber_attacks: https://www.researchgate.net/profile/Wiem-Tounsi/publication/320027747_A_survey_on_technical_threat_intelligence_in_the_age_of_sophisticated_cyber_attacks/links/59fc7cb70f7e9b9968bd9e02/A-survey-on-technical-threat-intelligence-in-the-age-of-sophisticated-cyber-attacks.pdf

Anexos

Anexo 1. Instrumento de evaluación de la aplicabilidad de Ciber Kill Chain

Nombre de la empresa

Instrumento de la evaluación de la aplicabilidad de Cyber Kill Chain

Evaluación de la Aplicabilidad Cyber Kill Chain

Tabla de Contenidos

Versiones

Versión	Actualizado por	Fecha de Modificación	Descripción del cambio
1.0	Jurguen Kirton	24/10/2021	Creación del documento

Resumen

Este documento es un instrumento para la evalaución de la aplicabilidad del modelo Cyber Kill Chain en las empresas.

Nivel de Implementación Cyber Kill Chain		
0	Inexistente	La fase o la etapa no se ha aplicado y no existe ninguna estrategia relacionada que se haya aplicado
1	Inicial	La fase o la etapa ha sido considerada por la organización por lo que se encuentra en un etapa inicial, sin embargo, no se ha comenzado a desarrollar
2	En proceso	La fase o la etapa se encuentra en un proceso de desarrollo
3	Implementado	La fase o la etapa se ha logrado implementar, sin embargo, no se ha desarrollado y no ha a alcanzado un nivel de madurez alto
4	Avanzado	La fase o la etapa ha logrado alcanzar cierto nivel de madurez con respecto a su implementación, sin embargo, no ha alcanzado su nivel máximo
5	Completado	La fase ola etapa se ha logrado implementar en su completitud

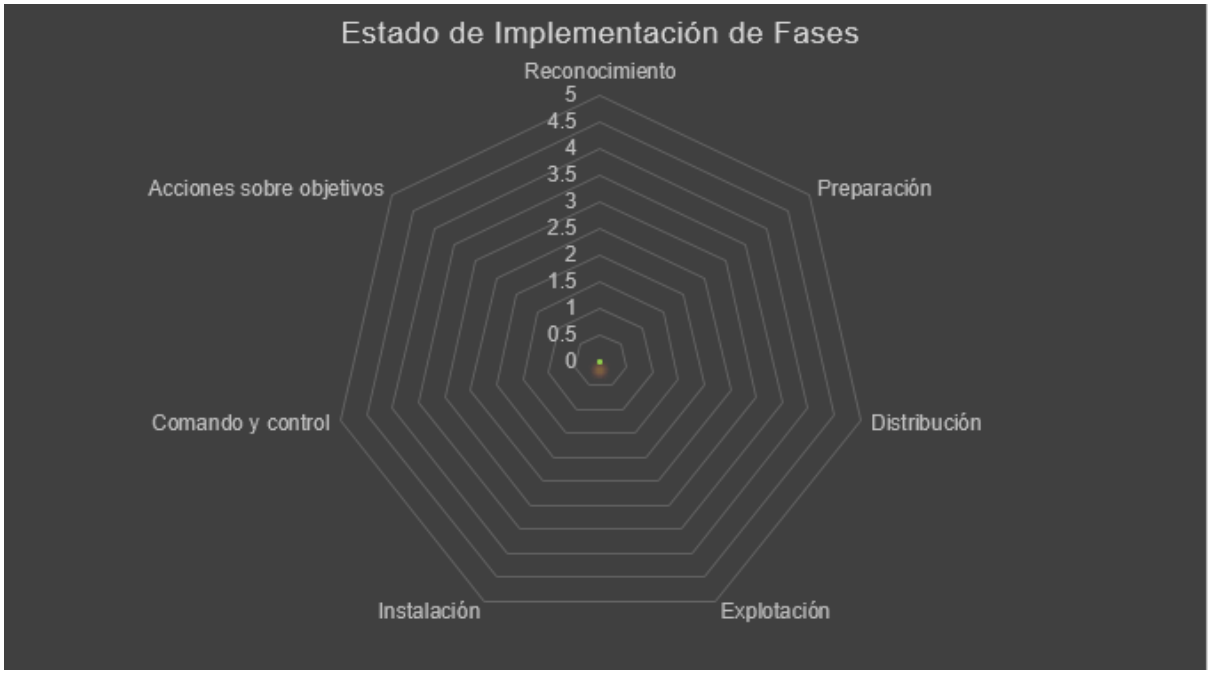
Análisis Nivel de Implementación Cyber Kill Chain			
Etapas y Fases	Preguntas	Respuestas	
Etapa de pre compromiso		Sí	No
Reconocimiento	¿Existen mecanismos para la protección de información pública de la organización que pueda revelar datos confidenciales?		
	¿Existen mecanismos para el control de perfiles completos sobre la organización en la		
	¿Existe información confidencial expuesta al público?		
	¿La información de los sistemas que componen la infraestructura de TI de la organización es difícil de obtener?		
	¿Existen mecanismos de control para la protección de los nombres de dominio?		
	¿Los sitios web de la empresa implementan mecanismos de seguridad?		
	¿Los puertos de los diferentes servidores y sistemas están protegidos?		
	¿Existen mecanismos control de anti spam?		
	¿La organización implementa políticas para mitigar o evitar el phishing?		
	¿La organización implementa controles de seguridad orientados a la ingeniería social?		
	¿La organización implementa mecanismos de analítica web?		
	¿La organización implementa políticas orientadas a la regulación de la información que se publica en la web?		
	¿La organización implementa firewalls en su infraestructura?		
	¿La organización implementa sistemas de prevención intrusiones?		
	¿La organización implementa mecanismos de autenticación?		
	¿Existen políticas de control sobre el uso de las redes sociales?		
	¿En caso de publicarse información que debe mantenerse pública, se aplican métodos de cifrado de la información para impedir accesos no autorizados?		
	¿En caso de utilizar servicios públicos en la nube, la información que maneja está protegida, o bien, es información que no revela datos importantes sobre la compañía?		
	¿La organización implementa mecanismos orientados a proteger perímetro más externo de la red?		
	¿La organización conoce todos los puntos de entrada de los diferentes sistemas?		
Preparación	¿La organización implementa mecanismos de control y trazabilidad de puertas traseras?		
	¿La organización implementa mecanismos de control y trazabilidad para el acceso remoto?		

Distribución	¿La organización implementa un programa de concientización sobre ingeniería social?		
	¿La organización implementa sistemas de detección y de filtro de correos maliciosos?		
	¿La información de los empleados no se encuentra expuesta como para recibir información que no sea de competencia para la compañía?		
	¿La información de identidad de los usuarios o empleados se encuentra protegida?		
	¿Existen datos de la organización que puedan ser difícilmente enmascarados?		
	¿Se implementa algún mecanismo de control para evitar el enmascaramiento de datos o información de la organización?		
	¿Existen mecanismos para contrarrestar la descarga de archivos, en cualquier formato existente, no autorizados o sospechosos?		
	¿Existen mecanismos o medidas para la protección de los medios físicos usb?		
	¿Se implementan mecasnimos para evitar o contrarrestar vulnerabilidades a nivel de DNS?		
	¿Se implementan mecanismos de captura de paquetes para el análisis de red?		
	¿Existe un control exhaustivo sobre el tráfico de red de la organización?		
	¿Existen métodos para medir los niveles de implementación de los programas de concientización?		
Etapa de compromiso			
Explotación	¿Los sistemas operativos y el software que se utiliza en la organización son seguros?		
	¿Los sistemas operativos y el software que se utiliza en la organización son debidamente mantenidos?		
	¿Se implementa software anti virus en los diferentes equipos de los empleados?		
	¿Existen mecanismos de control para el acceso remoto por medio de consola?		
	¿La organización cuenta con mecanismos de seguridad para exploits?		
	¿La organización cuenta con mecanismos de seguridad para ataques de denegación de servicios?		
	¿La organización cuenta con mecanismos de seguridad para la protección de explotaciones a nivel de protocolos (FTP, SMTP, NTP, SSH, entre otros)?		
	¿La organización cuenta con mecanismos de seguridad contra ataques dirigidos a la administración de la memoria de los diferentes equipos?		
	¿La organización cuenta con sistemas de detección de intrusos en la red?		
	¿Existen mecanismos para la detección de anomalías en los datos entrantes y salientes de la red de la organización?		
	¿La organización da un seguimiento sobre las detecciones o monitores que se realizan a nivel de los sistemas?		
	¿La organización hace uso de indicadores de compromiso así como de otros indicadores con el fin de mejorar el proceso de análisis en las detecciones y el monitoreo?		
	¿La acciones de las detecciones o monitoreo que se realiza están automatizadas?		
	¿La organización implementa mecanismos de registro de logs de los diferentes sistemas?		
	¿La organización implementa una política de retención de registros de logs?		
	¿La organización implementa mecanismos para la correlación de eventos o registros logs?		

Instalación	¿Existen controles de seguridad a nivel de los equipos de los usuarios que eviten la instalación ejecución de software malicioso?		
	¿La configuración en los equipos evita que los usuarios, aplicaciones o servicios puedan ejecutar tareas sin autorización de la organización?		
	¿Existen mecanismos de seguridad que eviten que se inicien aplicaciones o servicios de manera automática al iniciar los equipos de los usuarios o empleados?		
	¿Existen mecanismos para el tratamiento de amenazas críticas como el ransomware?		
	¿Existen sistemas de respaldo que faciliten la recuperación de la información en caso de pérdida de la misma?		
	¿Se realiza un análisis de malware en sospechas malware?		
Etapa de post compromiso			
Comando y control	¿Existen mecanismos de seguridad que eviten la exfiltración de la información de la organización?		
	¿Existen mecanismos de control para evitar la comunicación de los sistemas de la organización con servidores externos maliciosos?		
	¿Existen mecanismos para interrumpir accesos o comunicaciones remotas no permitidas?		
	¿Existen mecanismos para filtrar las direcciones IP y los protocolos HTTP?		
	¿Se implementan mecanimos de seguridad que permitan limitar las solicitudes HTTP?		
	¿Existen mecanismos para detectar actividad inusual en las cuentas de los usuarios?		
Acciones sobre objetivos	¿Los sistemas de la organización son interdependientes o se implementan mecanismos de seguridad que eviten ataques masivos sobre los distitntos sistemas de la organización?		
	¿Existen mecanismos para evitar que los sitemas de la organización se puedan utilizar para ataques basados en botnets?		
	¿Existen controles que eviten el control directo sobre los diferentes equipos o sistemas de la organización?		
	¿Las credenciales de los sistemas y de los usuarios están debidamente protegidas?		
	¿Se implementan sistemas de seguridad que permitan la detección o revisión de proxies?		
	¿Se implementan firewalls basados en lista de control de acceso?		
	¿Se implementa una infraestructura basada en honeypots?		

Datos Estadísticos de las Fases

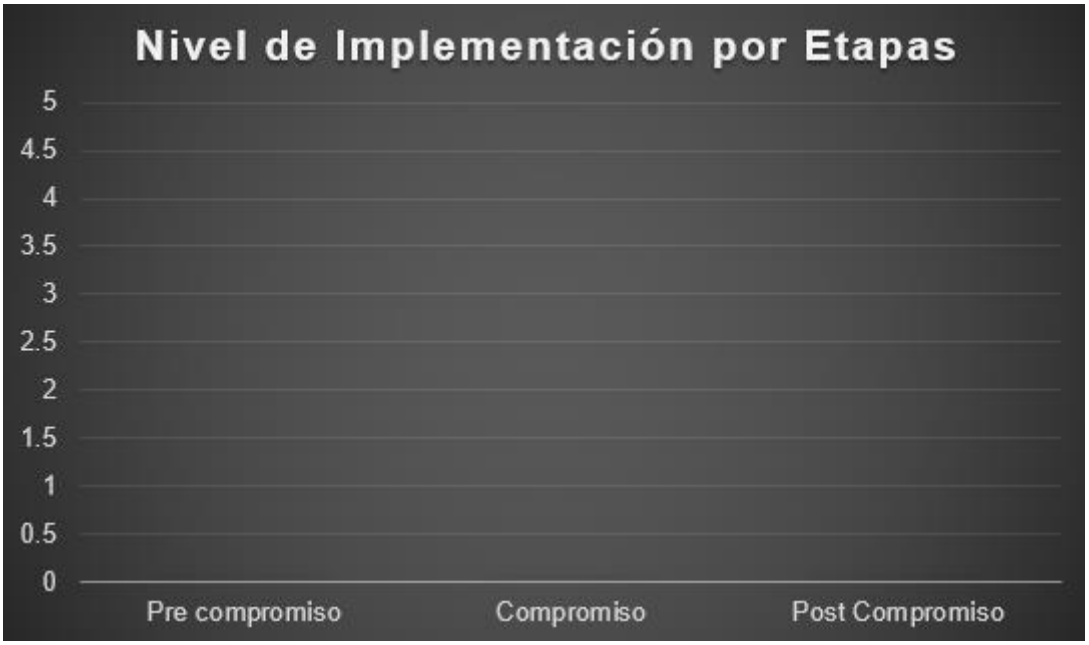
Fases	Total Preguntas	Resultados Afirmativos	Resultados Negativos
Reconocimiento	20	0	0
Promedio Reconocimiento		0	0
Nivel de Implementación		0	0
Preparación	2	0	0
Promedio Preparación		0	0
Nivel de Implementación		0	0
Distribución	12	0	0
Promedio Distribución		0	0
Nivel de Implementación		0	0
Explotación	16	0	0
Promedio Explotación		0	0
Nivel de Implementación		0	0
Instalación	6	0	0
Promedio Instalación	N/A	0	0
Nivel de Implementación		0	0
Comando y control	6	0	0
Promedio Comando y control		0	0
Nivel de Implementación		0	0
Acciones sobre objetivos	7	0	0
Promedio Acciones sobre ob		0	0
Nivel de Implementación		0	0


Estado de Implementación de Fases
Reconocimiento
5
4.5
4
3.5
3
2.5
2
1.5
1
0.5
0
Preparación
Distribución
Explotación
Instalación
Comando y control
Acciones sobre objetivos


Nivel de Deficiencia de Implementación de Fases
5
4.5
4
3.5
3
2.5
2
1.5
1
0.5
0
Reconocimiento
Preparación
Distribución
Explotación
Instalación
Comando y control
Acciones sobre objetivos

Datos Estadísticos de las Etapas

Etapas	Total Preguntas	Resultados Afirmativos	Resultados Negativos
Pre compromiso	34	0	0
Promedio Pre Compromiso		0	0
Nivel de Implementación		0	0
Compromiso	22	0	0
Promedio Compromiso		0	0
Nivel de Implementación		0	0
Post Compromiso	13	0	0
Promedio Post Compromiso		0	0
Nivel de Implementación		0	0


Nivel de Implementación por Etapas
5
4.5
4
3.5
3
2.5
2
1.5
1
0.5
0
Pre compromiso
Compromiso
Post Compromiso


Estado de Implementación por Etapas
Pre compromiso
5
4
3
2
1
0
Post Compromiso
Compromiso


Nivel de Deficiencia de Implementación por Etapas
5
4.5
4
3.5
3
2.5
2
1.5
1
0.5
0
Pre compromiso
Compromiso
Post Compromiso


Estado de Deficiencia de Implementación por Etapas
Pre compromiso
5
4
3
2
1
0
Post Compromiso
Compromiso

Análisis Nivel de Implementación Cyber Kill Chain		
Etapas y Fases	Nivel de Implementación Positivo	Nivel de Implementación Negativo
Etapa de pre compromiso	0	0
Reconocimiento	0	0
Preparación	0	0
Distribución	0	0
Etapa de compromiso	0	0
Explotación	0	0
Instalación	0	0
Etapa de post compromiso	0	0
Comando y control	0	0
Acciones sobre objetivos	0	0

Niveles de Implementación de Cyber Kill Chain	
Valores Cuantitativos	Valores Cualitativos
0	Inexistente
1	Inicial
2	En proceso
3	Implementado
4	Avanzado
5	Completado

Análisis Nivel de Implementación Cyber Kill Chain

Etapas	Recomendaciones
Etapa de pre compromiso	
Reconocimeinto	Controlar los sistemas de acceso a las plataformas
	Considerar la información que se publica o se comparte a través de diferentes medios
	Implementar mecanismos de cifrado de la información para impedir accesos no autorizados
	Invertir en métricas de detección de malware
	Considerar la seguridad desde la perspectiva del atacante para tener un conocimiento más exacto sobre cómo implementar medidas de seguridad
	Aplicar pruebas periódicas de exploración y penetración externas
	Aplicar procesos de inteligencia de amenazas durante los ensayos o pruebas de penentración
	Implementar sistemas los cuales se encarguen de recopilar los registros de los usuarios que acceden a los diferentes sistemas y aplicaciones , y generar las alertas necesarias para la idenitificación rápida y precisa de usuarios no deseados
	La organización de aplicar procedimientos de análisis detallado sobre la información que se hace pública
	La organización debe considerar todos los posibles ataques que se puedan generar, esto con el fin de lograr detener los ataques lo más antes posible
	Los empleados deben tener la capacidad de verificar y reconocer al personal de la organización, desechar y destruir de forma segura documentos que contengan información confidencial
	Se debe implementar procesos de análisis web, Inteligencia de amenazas y considerar la implementación de sistema de detección de intrusiones en la red
	La organización debe considerar implmentar una política para el intercambio de la información
	Se debe considerar el uso de listas de control de acceso
Preparación	Invertir en la formación y capacitación de los empleados en temas de seguridad de la información, y mantener una cultura organizacional basada en la ciberseguridad
	Aplicar proceso de análisis para comprender los artefactos de compromiso de los malwares actuales
	Crear procedimientos para la detección temprana de malware en donde se pueda considerar archivos y metadatos que sean recopilados para poderlos analizar más adelante y detectar nuevos ataques
	La organización debe mantenerse actualizada sobre las vulnerabilidades que se vayan descubriendo
	Mantener actualizados los sistemas y aplicar los parches necesarios
	Se deben de aplicar procesos de inteligencia de amenazas y considerar sistemas de detección de intrusiones en la red
	se debe de considerar la implementación de sistemas de prevención de intrusiones en la red
Distribución	Los empleados deben ser capaces de responder ante un ataque a través de la identificación de los mismos y saber qué hacer en caso de que suceda un incidente u ocurra un ataque
	Implementar métricas de rastreo y trazabilidad para investigar a fondo el tipo de ataque y analizar la información de la organización que ha sido comprometida
	La organización debe analizar qué medios de transmisión se utilizan en los intentos de intrusión y cuáles sistemas y empleados o clientes son objetivos del ataque
	La organización debe ser capaz de detectar las cargas útiles que se generan en los medios transmisión
	La organización debe de implementar las medidas de protección técnicas para el uso de medios de almacenamiento físicos
	Se debe implementar diferentes capas de seguridad, en donde se considere la infraestructura necesaria de equipos para la protección de la información
	Se debe de considerar la protección contra malware a nivel de endpoints
	Deben existir procedimientos de administrar de cambios
	Se debe de implementar listas blancas de aplicaciones
	Considerar filtros de proxy y sistemas de prevención de intrusiones basado en host
	Considerar la implementación de antivirus en línea
	Contiene: Listas de control de acceso de enrutadores; Cortafuegos compatible con aplicaciones; Zonas de confianza; Sistema de detección de intrusiones de red entre zonas
	Se debe considerar la implementación de servicios de seguridad de la información orientados a la protección como la protección avanzada contra amenazas (ATP)

Etapa de compromiso	
Explotación	Proteger los datos y la información a través del respaldo y parcheo de datos
	Mantener actualizados los equipos y los sistemas de protección
	Aplicar de forma periódica copias de seguridad para evitar la pérdida total de los datos
	Considerar el uso de parches y aplicar escaneos automáticos de vulnerabilidades
	Considerar la formación sobre el desarrollo de software seguro
	La organización debería utilizar o implmentar un SIEM para análizar los registros y otros análisis para identificar estas actividades maliciosas
	La organización debe considerar la protección sobre programas y servicios que sean de importancia para los sistemas
	Se debe de implementar de constraseñas seguras
	Se debe de aplicar y gestión de parches
	Disrupt: Prevención de ejecución de datos
	La organización debe considerar la integración o compatibilidad entre las aplicaciones con el firewall existente
	Se debe de considerar la implementación de sistemas de detección de intrusiones de red considerando zonas o los conjuntos de reglas predefinidas de los firewalls
Instalación	La organización debería de contar con herramientas de seguridad basadas en la detección de amenazas y respuesta sobre endppoints
	Se debe de monitorizar el estado de los sistemas
	Considerando las soluciones de seguridad de la información que la organización implementa, se puede realizar procesos de reconocimiento y registro de los procesos de instalación, y crear nuevas medidas de seguridad
	Aplicar correctas medidas de seguridad orientadas al control de acceso de los usuarios
	Se debe aplicar procesos de autenticación fuertes que limiten el acceso a la información
	En caso de que se genere una alerta o exista una sospecha de la instalación de software o herramientas maliciosas, se debe aplicar un proceso inmediato de recuperación de datos a partir de las copias de seguridad y restaurar los servidores a un estado limpio
	La organización debe considerar la implementación de certificados de seguridad que ayuden a idenitificar todos aquellos programas, aplicaciones y servicios que son autenticos
	Se debe de aplicar procesos para la gestión de eventos así como para la información de seguridad
	La organización debe de hacer uso de contraseñas seguras y aplicar procesos de autenticación de dos factores
	La organización debe de considerar la delegación segura de privilegios de usuarios así como su separación
	La organización debe considerar la implementación y uso de listas de control de acceso sobre enrutadores

Etapa de post compromiso	
Comando y control	La organización debe ser capaz de detectar los ataques y con base a la información sobre del mismo así como conbase a información de contexto deberías ser también capaz de rastrear el ataque hasta lograr identificar al atacante
	Se debe implementar sistemas de detección de intrusos para la detección de anomalías
	Se debe de dehabilitar todas las conexiones a las redes o sistemas que estén siendo vulnerados
	Se debe de monitorear el tráfico de red así como analizar los volumenes de datos que se generan a través de la misma y generar alertas cuando se excedan ciertos umbrales
	La organización debe de utilizar inteligencia de amenazas para detectar comportamientos insuales
	La organización debe tener la capacidad de detectar todas aquellas vulnerabilidades a nivel de los sistemas con el fin de mitigar el riesgo
	La organización debe considerar segmentar la red interna, esto en caso de que no se mantenga una infraestructura de red basada en segmentación
	La organización debe de implementar controles basados en el redireccionamiento del sistema de nombres de dominio
Acciones sobre objetivos	La organizaón debería de considerar la reconfiguración de los cortafuegos de la red empresarial
	Se debe de implementar sistemas de honeypots que coadyuven a la salvaguarda de la información
	Se debe de monitorizar la actividad de las comunicaciones que ocurren a nivel de la red
	La organización puede considerar de aplicar procesos de informática forense que ayuden a la evaluación y reconstrucción de
	La organización debe ser capaz de conocer que medidas se deben de tomar o valorar por lo que también se debe de considerar de antemano la delegación de responsabilidades por parte del personal encargado de la seguridad de la información de la empresa así como sobre los procesos técnicos relevantes
	La organización debe considerar estrategias basadas en cifrado y encriptado en reposo así como en tránsito
	La organización debe ser capaz de dar respuesta oportuna a los diferentes ataques o incidentes generados por estos
	La organización debe de asgurar la disponibilidad de los servcios de TI sin importar el nivel de impacto del incidente de seguridad
	Se debe de monitorear la actividad de la base de datos e identificar todas aquellas actividades sospechosas