CIBERSEGURIDAD: METODOLOGÍA APROXIMADA PARA REALIZAR INVESTIGACIÓN EN INTELIGENCIA CIBERNÉTICA

Technical Report · May 2020

DOI: 10.13140/RG.2.2.25127.37289/2

1 author:

Emanuel Ortiz
Red de Investigación Academica en Ciberseguridad
26 PUBLICATIONS **27** CITATIONS

SEE PROFILE

CIBERSEGURIDAD: METODOLOGÍA APROXIMADA PARA REALIZAR INVESTIGACIÓN EN INTELIGENCIA CIBERNÉTICA

Presentación de la Red de investigación Académica

La Red de Investigación en Cibercrimen y Ciberseguridad "*RedCiber*" realiza un trabajo colaborativo a través de sus nodos de cooperación académica, los cuales trabajan en diferentes líneas de investigación y apoyan el trabajo de los otros nodos construyendo datos de alta importancia para investigadores de las ciencias forenses y áreas afines a la informática, Ciberseguridad, Cibercrimen y la Cibercriminologia.

El concepto y creación de la Red de Investigación en Ciberseguridad y Cibercrimen "*RedCiber*" en alianza de la Asociación Internacional de Informática Forense, tiene como objeto difundir, ampliar y reconocer a los expertos en estas áreas fundamentales para la Seguridad Digital, sin desconocer la interdisciplinariedad o multidisciplinariedad que debe responder a las necesidades actuales de la seguridad de forma integral.

Abstract

La inteligencia cibernética y las habilidades de un investigador en ciberseguridad y de inteligencia de amenazas, están estructurados en el conocimiento de su entorno, por ende, es importante el contexto de la organización, y para la función que desempeña dentro del equipo técnico de seguridad, la necesidad de poder desarrollar estrategias, técnicas, y procedimientos para emplear actividades en pro de determinar, identificar y establecer el origen de una amenaza, riesgo y vulnerabilidad cibernética, por ello es importante tener una metodología que le permita garantizar esos lineamientos futuros como especialista en seguridad informática y de la información.

Palabras Clave: *Seguridad en la Información, Cibercrimen, inteligencia de amenazas, Gestión de Riesgos, Amenazas Cibernéticas, Seguridad Nacional.*

Antecedentes

Los hechos por medio del tiempo han sido evidentemente complejos en materia de Ciberseguridad; algunos de ellos los señala (Ortiz Ruiz, 2019) en los orígenes del Cibercrimen, sin embargo es importante elevar estas connotaciones y divisiones a través de los avances tecnológicos de la humanidad; si bien es cierto este fenómeno hace parte de un título grande y contextualizado en un todo, estas afectaciones a la ciberseguridad y Seguridad Digital tuvieron nacimiento mucho más antes de lo que imaginamos, por ende la importancia y lugar de relevancia que tiene para muchos sectores de la Economía. Uno de ellos, es brindar unos aspectos centrales y estandarizados para poder focalizar los puntos de acción e instrumentalizar todos los elementos de investigación que la industria exige en esta materia.

CIBERSEGURIDAD: METODOLOGÍA APROXIMADA PARA REALIZAR INVESTIGACIÓN EN INTELIGENCIA CIBERNÉTICA

Para comprender la funcionalidad de la inteligencia de amenazas cibernéticas y su enfoque estructurado en la ciberseguridad; debe partir de un punto de vista académico, y se puede iniciar a partir de conocer la participación del ciberespacio como eje temático fundamental y posterior a ello, entender la forma como el cibercrimen puede afectar la ciberseguridad a partir de lo que conocemos actualmente como ciberamenazas y los riesgos cibernéticos. Como se determinó anteriormente el "Ciberespacio" interactúa fielmente sobre este desarrollo conceptual y practico de la ciberseguridad.

En ese orden de ideas, es importante definir las causas históricas desde hace 3 años el ciberataque ocasionado en Ucrania y los eventos más recientes ocurridos, aquellos hechos fueron relacionados con una serie esquemas de vulnerabilidades que empezaron a visibilizarse el 27 de junio de 2017, empleando el malware Petya, el cual afectó varios sitios web de instituciones y empresas ucranianas, incluyendo bancos, ministerios, diarios y empresas de electricidad (Wikipedia, 2020). Se recibieron reportes de infecciones similares de Francia, Alemania, Italia, Polonia, Rusia, Reino Unido, los Estados Unidos y Australia. Del mismo modo, ESET indicó que el 80% de todas las infecciones procedían de Ucrania, siguiéndole Alemania con aproximadamente un 9% de las infecciones. El 28 de junio de 2017, el gobierno ucraniano declaró que el ataque fue frenado. El 30 de junio de 2017, la Associated Press informó que los expertos concluyeron que [1]Petya había dado su aviso tiempo atrás frente a diferentes vulnerabilidades aprovechadas por los ciberdelincuentes.

Los diferentes sistemas de defensa, entre ellos los relacionados con ciberseguridad mundial también fueron advertidos y alertados frente a las diferentes consecuencias que pudo materializar en los diferentes sectores, así como se pudo evidenciar posteriormente su carencia de recuperación activa de los sistemas o plataformas afectadas.

La actualización de sistemas operativos, infraestructuras que puedan ser afectadas mediante un camino más corto para el ciber terrorista o cibercriminal, es vital entender la problemática que se extiende y en el cual se personalizan estos ataques, estos fenómenos no esperan que el sistema se encuentre en construcción, desarrollo o se despliegen mejoras en el mismo. En virtud de esto se concibe la importancia de anticipar mediante inteligencia cibernética, y en este caso de ciberseguridad y riesgos, debe conducir a realizar análisis sobre esas amenazas que pueden afectar los tres pilares de la información y su custodia.

[1] Petya: Es un *malware* de tipo *ransomware* reportado por la empresa Heise Security. Petya se esparce como troyano usando el popular sistema de archivos en la nube Dropbox.[1] Mientras la mayoría de los malware de secuestro de computadoras selecciona los archivos a encriptar, Petya aumenta el daño potencial al impedir el arranque de la computadora .Tomado de: https://es.wikipedia.org/wiki/Petya_(malware)

CIBERSEGURIDAD: METODOLOGÍA APROXIMADA PARA REALIZAR INVESTIGACIÓN EN INTELIGENCIA CIBERNÉTICA

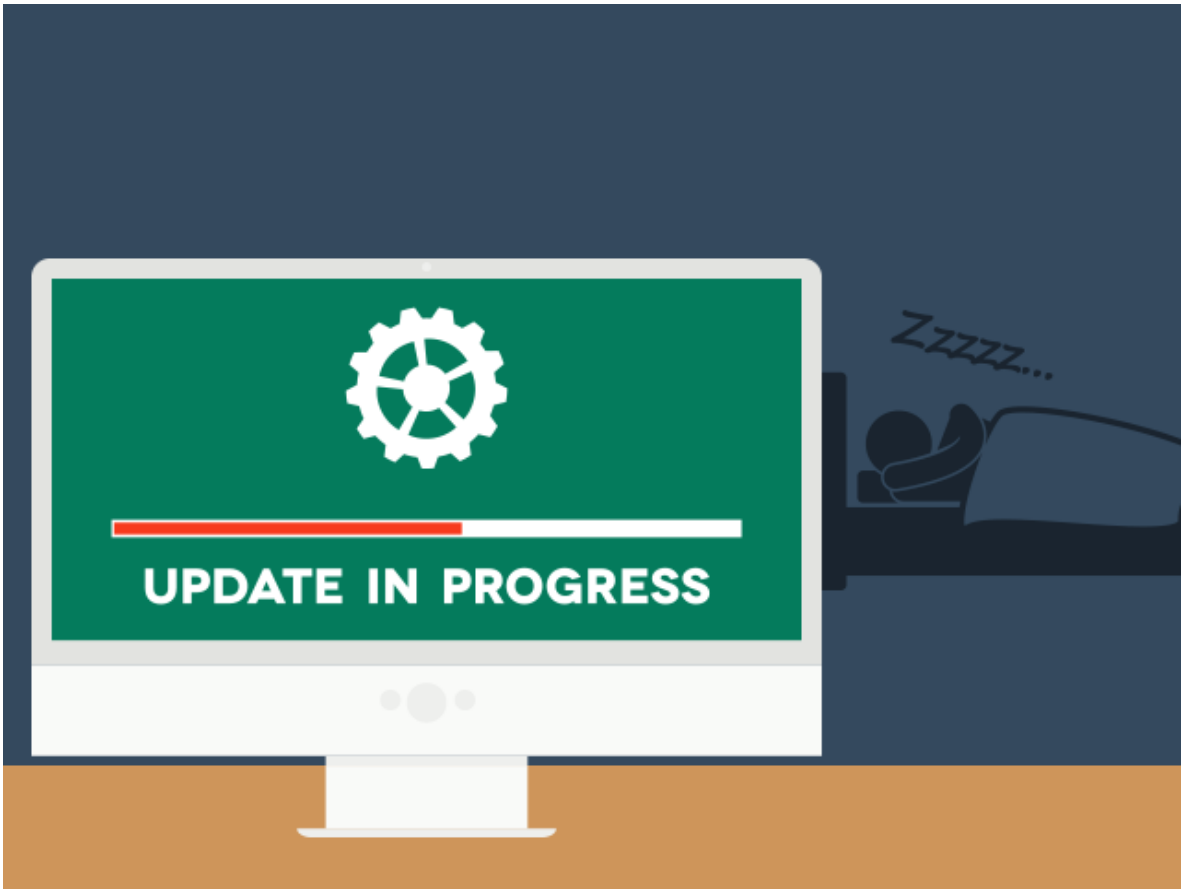


Figura ilustrativa tomada: Google Update

Mientras se realizan actividades de defensa y de protección en las infraestructuras críticas de un país, se debe conocer y anticipar a su posible contexto, asimismo lo ha indicado el marco de trabajo [2]NIST, por medio de su versión (Instituto Nacional, 2020) en la cual establece la importancia de los (ICS) que en inglés se traduce, Sistemas de Control Industrial, los (CPS) Cyber -Physical Systems y los dispositivos conectados en general como, Internet de las Cosas (IoT). En ese panorama el marco de

[2] Instituto de Estándares Tecnológicos de los Estados Unidos: El **Instituto Nacional de Estándares y Tecnología** (**NIST** por sus siglas en inglés, *National Institute of Standards and Technology*), llamada entre 1901 y 1988 **Oficina Nacional de Normas** (**NBS** por sus siglas del inglés *National Bureau of Standards*), es una agencia de la Administración de Tecnología del Departamento de Comercio de los Estados Unidos. La misión de este instituto es promover la innovación y la competencia industrial en Estados Unidos mediante avances en metrología, normas y tecnología de forma que mejoren la estabilidad económica y la calidad de vida. https://es.wikipedia.org/wiki/Instituto_Nacional_de_Est%C3%A1ndares_y_Tecnolog%C3%ADa

trabajo define 5 prácticas esenciales para la creación de escenarios de Ciberseguridad para las organizaciones, así:

1. Describir la postura actual de su Ciberseguridad
2. Definir su estado objetivo de Ciberseguridad
3. Identificar las oportunidades priorizadas para mejorar dentro un proceso continuo y repetible
4. Evaluar hacia el estado" objetivo"
5. Comunicarse entre los interesados **internos y externos** sobre el riesgo de Ciberseguridad.

Bajo este mismo esquema se plantea el marco de trabajo NIST, un panorama que pretende describir su marco actual de ciberseguridad, definir el alcance. Identificar esas oportunidades priorizadas para mejorar mediante un proceso continuo, enfocado en la estrategia principal y con una continua evaluación para identificar realmente el riesgo de la organización.

En la coyuntura de algún riesgo, siempre es importante examinar su contexto, en lo que tiene que ver con el panorama o tendencia hacia detectar nuevas oportunidades para adelantar inteligencia cibernética, por ejemplo: Covid19[3], situación mundial que ha marcado la pauta frente a nuevas amenazas emergentes y lo relacionado con transformación digital que hoy por hoy viene tomando fuerza.

Como lo describe actualmente NIST, una amenaza avanzada persistente consta de lo siguiente:

Es un adversario que posee niveles sofisticados de experiencia e importantes recursos que le permiten crear oportunidades para lograr sus objetivos utilizando múltiples vectores de ataques (por ejemplo, cibernéticos, físicos y engaños). Estos objetivos, normalmente, incluyen establecer y extender las bases dentro de la infraestructura de TI de las organizaciones objetivo, con el propósito de extraer información, perjudicar o dificultar los aspectos críticos de una misión, programa u organización; o posicionarse para llevar a cabo estos objetivos en el futuro. La amenaza persistente avanzada:

- *persigue sus objetivos reiteradamente durante un período prolongado de tiempo;*
- *se adapta a los esfuerzos realizados por el defensor para resistir el ataque; y*
- *está decidida a mantener el nivel de interacción necesario para conseguir sus objetivos.*

[3] La **COVID-19**[nota 2] (acrónimo del inglés *coronavirus disease 2019*),[4] también conocida como **enfermedad por coronavirus**[3], e incorrectamente como **neumonía por coronavirus**, es una enfermedad infecciosa causada por el virus SARS-CoV-2

CIBERSEGURIDAD: METODOLOGÍA APROXIMADA PARA REALIZAR INVESTIGACIÓN EN INTELIGENCIA CIBERNÉTICA

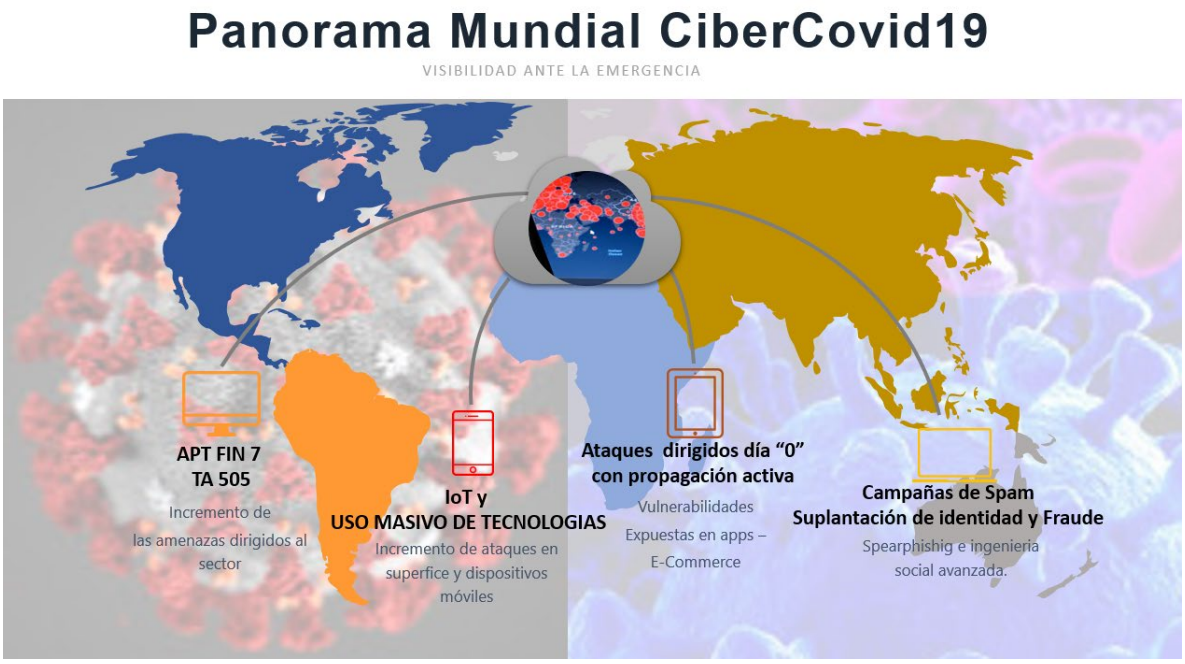


Figura elaborada por el autor

Como se observa en la anterior gráfica las amenazas avanzadas persistentes llamadas así, en complemento en lo manifestado por NIST, se miden por su impacto y posibilidad de ataque son muchas veces subestimadas, las cuales pueden impactar un sector en particular (*Gobierno, salud industrial, retail, comercio o financiero*), particularmente cuando se habla de las [4]APT´s, las cuales cumplen con varios factores que permiten estrictamente asociar nuevos escenarios tecnológicos. En ese orden de ideas muchos de los factores que generan un riesgo o una posible amenaza pueden estar vinculados entre sí.

Para el caso en particular, CiberCovid19 como se ha definido en el argot popular, ha desarrollado un sin número de escenarios que facilitan la interacción de las APT´s, que particularmente están contagiando de manera apresurada y sobre todo, enfocado en diferentes escenarios que tienen presencia política, económica y sobre todo tecnológica; a pesar de todo ello, estos grupos cibercriminales poseen un método de transferencia único, anónimo y expuesto frente a diferentes

[4] **APT:** Una **amenaza persistente avanzada**, también conocida por sus siglas en inglés, **APT** (por ***Advanced Persistent Threat***), es un conjunto de procesos informáticos sigilosos orquestados por un tercero (organización, grupo delictivo, una empresa, un estado,...) con la intención y la capacidad de atacar de forma avanzada (a través de múltiples vectores de ataque) y continuada en el tiempo, un objetivo determinado (empresa competidora, estado,...). Este malware es instalado usando exploits que aprovechan vulnerabilidades de la máquina objetivo. Para realizar la infección es habitual aprovechar vulnerabilidades de día cero y/o ataques de abrevadero.

CIBERSEGURIDAD: METODOLOGÍA APROXIMADA PARA REALIZAR INVESTIGACIÓN EN INTELIGENCIA CIBERNÉTICA

esquemas de organizaciones, Europol mediante (EC3, 2019) informe ha expuesto 5 metodologías en las cuales el cibercrimen puede afectar a los ciber ciudadanos o victimas hiperconectadas

- Phishing/smishing/vishing
- Business email compromise
- Bulletproof hosting
- Herramientas de anonimización
- Abuso del uso de las Criptodivisas

Estos escenarios frente a la pandemia Covid19 se han estructurado frente a la anterior gráfica en cuatro escenarios fundamentales:

- **Grupos Cibercriminales enfocados en Amenazas Avanzadas Persistentes** Ej: [5]Fin7, Carbanak y TA505: los grupos cibercriminales conocidos por medio d ela pandemia han aprovechado por abastecerse de nuevas y sofisticadas herramientas, algunas ya conocidas y otras descubiertas recientemente en el mundo de la web oscura o Darkweb.

- **Amenazas frente a dispositivos conectados o hiperconectados** ([6]IoT y dispositivos móviles): El complejo mundo de la tecnología hiperconectada, es el escenario perfecto para que atacantes de diferentes partes del planeta , estén estrictamente relacionados con la compra de productos y *Crime as a Sevice*, el cual denota un creciente mercado relacionado con el incremento de la compra de software maliciosos, sus siglas en ingles “Malware” que contiene capacidades para afectar tecnología conectada a dispositivos en el hogar o en el trabajo.

[5] Carbanak es una campaña de estilo APT dirigida (pero no limitada a) instituciones financieras que se afirmó que fue descubierta en 2014 por la compañía de ciberdelincuencia rusa / británica Kaspersky Lab, quien dijo que había sido utilizada para robar dinero de los bancos. Se dijo que el malware Microsoft Windows se introdujo en sus objetivos a través de correos electrónicos de phishing. Se decía que el grupo de hackers había robado más de 900 millones de dólares, no solo de los bancos sino de más de mil clientes privados.

[6] Internet de las Cosas: El **internet de las cosas** (en inglés, *Internet of Things*, abreviado *IoT*;IdC, por sus siglas en español [2]es un concepto que se refiere a una interconexión digital de objetos cotidianos con internet.Es, en definitiva, la conexión de internet más con objetos que con personas.También se suele conocer como *internet de todas las cosas* o *internet en las cosas*. Si los objetos de la vida cotidiana tuvieran incorporadas etiquetas de radio, podrían ser identificados y gestionados por otros equipos de la misma manera que si lo fuesen por seres humanos

CIBERSEGURIDAD: METODOLOGÍA APROXIMADA PARA REALIZAR INVESTIGACIÓN EN INTELIGENCIA CIBERNÉTICA

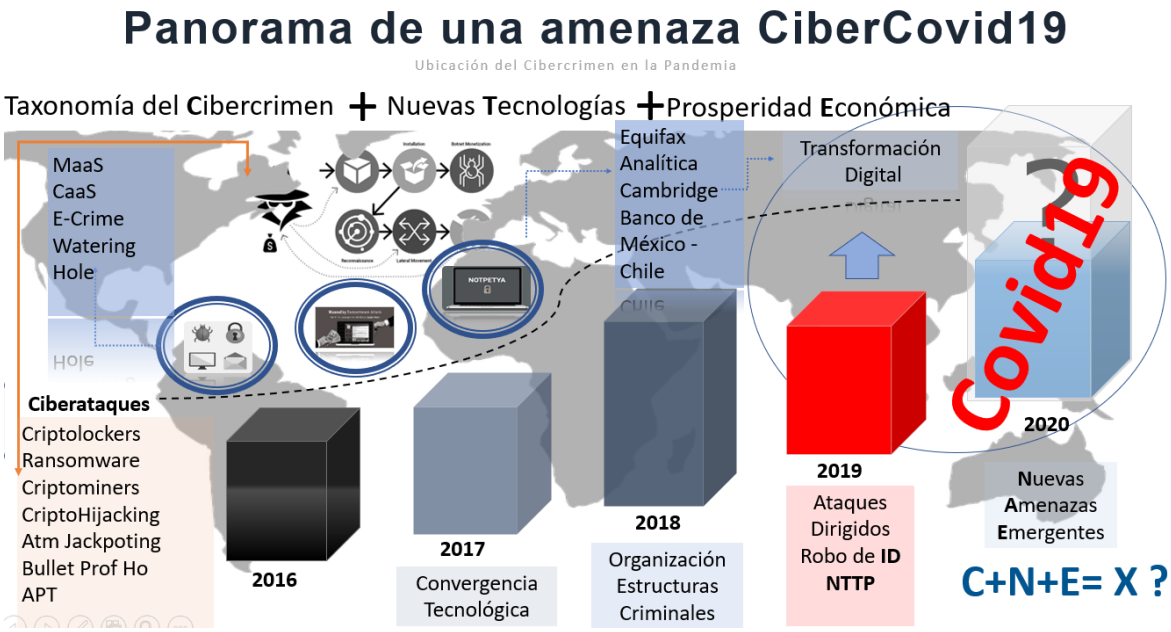
- **Aprovechamiento de vulnerabilidades día cero**: Estos escenarios están también ligados a la búsqueda constante de herramientas, como: Exploits que se trata de un software que permita atacar infraestructura relacionada con aquellas plataformas de uso cotidiano o masivo.

- **Campañas masivas de Spam y Spearphishing**: Ante este escenario, es importante destacar el uso de técnicas ya existentes y sobre todo con mucha actividad frecuente, sin embargo, son elementos que las organizaciones delincuenciales, no directamente asociado con organizaciones cibercriminales pueden afectar la imagen, reputación y buen nombre pequeñas, medias y grandes empresas. Por medio de Covid19 ha tenido un creciente incremento en lo que tiene que ver con la cantidad de señuelos dedicados a estas acciones.

Ahora bien, dentro del enfoque de la inteligencia cibernética es importante delimita ese contexto, situación política, económica y social de un sistema, estado, nación, gobierno, organizaciones y sobre todo las ventajas comerciales que esto radica constantemente.

CIBERSEGURIDAD: METODOLOGÍA APROXIMADA PARA REALIZAR INVESTIGACIÓN EN INTELIGENCIA CIBERNÉTICA

En la siguiente gráfica se indica el panorama global en ciberseguridad con diferentes tópicos y reflejos que tienen que ver con la evolución que ha tenido diferentes ataques relacionados con el el Cibercrimen, y lo conveniente de examinar cuales han sido los aspectos claves en estos escenarios de aplicabilidad de herramientas técnicas, operativas y estratégicas frente a estos escenarios. Por ello la importancia de vincular a las organizaciones diferentes mecanismos que permitan orientar la búsqueda directa de la prevención y la anticipación. Esto ajustado a los estándares conocidos y reflejados en este articulo:



Fuente: Elaborada por el Autor

En ese orden de ideas, es importante destacar la importancia en lo concerniente a determinar cuál es el objetivo de las diferentes Amenazas Persistentes bajo un panorama de riesgo; si bien es cierto, los diferentes ciberataques o ataques cibernéticos han podido trascender frente al uso de diferentes tecnologías y el abuso de estas; los diferentes adversarios se han transformado, en el 2016 los componentes eran los objetivos de alto valor, como: Sector financiero y Gubernamental, pero poco a poco fue cambiando la dinámica de infección y permanencia de estas amenazas. Hacia el 2018 las organizaciones criminales fijaron unos objetivos estratégicos formales, como lo fue el ataque al Banco de Chile y Banco de México. A partir de 2019 se ha venido transformando paulatinamente estas amenazas, considerándose hoy por hoy las consecuencias de no anticipar de manera activa frente a este tipo de riesgos. En la amenaza actualizada durante el Covid19 se realiza paulatinamente una transición obligada a la transformación digital, propiamente hablando y se

promulga diferentes actividades que remarcan nuevas amenazas emergentes; en ese sentido la pregunta abierta a desarrollar sería: *¿Se requiere de la inteligencia de cibernética para poder aproximarnos a esos riesgos y como mitigarlos?*

Cambio de enfoque que sugiere reformular el paradigma

Para la ciberseguridad o la seguridad cibernética es importante delimitar que actores y adversarios están enfocados realmente en los sectores, indicando que; la inteligencia de amenazas es una de las herramientas que permite enfocar esos esfuerzos. Dentro del informe que realizó ISACA (ISACA, 2013) en su página 13, en el cual se refiere a la amenaza avanzada persistente acuñada desde el 2005 asociada al ciberespionaje ocurridos en los EEUU cintra organismos del estado, pero la más adaptada, es la reconocida por el Instituto Nacional de Normas y Tecnología de EEUU, el cual enuncia lo siguiente:

Una APT es como un adversario que posee niveles sofisticados de experiencia e importantes recursos que le permiten crear oportunidades para lograr sus objetivos utilizando múltiples vectores de ataques (por ejemplo, cibernéticos, físicos y engaños). Estos objetivos, normalmente, incluyen establecer y extender las bases dentro de la infraestructura de TI de las organizaciones objetivo, con el propósito de extraer información, perjudicar o dificultar los aspectos críticos de una misión, programa u organización; o posicionarse para llevar a cabo estos objetivos en el futuro. La amenaza persistente avanzada:(i) persigue sus objetivos reiteradamente durante un período prolongado de tiempo;(ii) se adapta a los esfuerzos realizados por el defensor para resistir el ataque; y(iii) está decidida a mantener el nivel de interacción necesario para conseguir sus objetivos.

Esta definición se acopla a lo comentado anteriormente para poder enfatizar el contexto mediante el cual se presenta este tipo de ataques; de esta manera poder reevaluar la necesidad de poder determinar ¿Cuál es la importancia de investigar y analizar que objetivos persigue la organización cibercriminal?, ¿Cuáles son sus principales armas para poder realizar un ataque cibernético?, ¿Dónde se encuentra ubicada o localizada un APT?... Estos interrogantes están asociados a la inteligencia cibernética y la metodología aplicada para su estudio y análisis.

Como el ejemplo en particular, la pandemia Covid19 cuyo contexto relaciona la oportunidad y las victimas hiperconectadas, como se manifiesta en la Aproximación del Cibercrimen redactado y escrito por (*Ortiz Ruiz, LIBRO SOBRE A APLICAO PRACTICA DA INVESTIGACAO CRIMINAL TECNOLOGICA, 2020*), es relevante enfatizar sobre las principales causas que se derivan de este estudio, a partir de una aproximación que permita focalizar los intereses de las organizaciones, los estados y las naciones para poder buscar el sentido de estas amenazas cibernéticas.

CIBERSEGURIDAD: METODOLOGÍA APROXIMADA PARA REALIZAR INVESTIGACIÓN EN INTELIGENCIA CIBERNÉTICA

Ejemplarizando el ciberataque a Ucrania ocurrido en el año 2017, y los recientes hechos descubiertos y expuestos en plataformas vulnerables hacia Eternal blue7, en donde por medio de vulnerabilidades expuestas hacia MS17010 y MS170 012. Este ciberataque no solamente dejó perdidas en ciberseguridad a nivel mundial, sino que también pérdidas económicas que superaron los 10 millones de dólares.

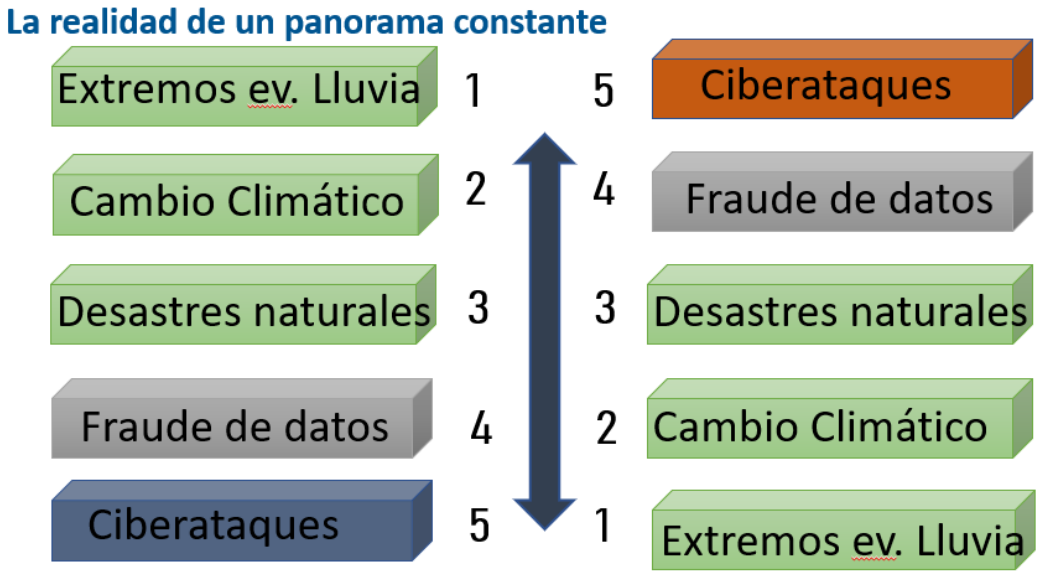
Mediante esta aproximación de la inteligencia cibernética se pretende recrear un contexto mediante el cual se pueda establecer unas pautas para poder utilizar la inteligencia de amenazas para poder enfatizar y acrecentar los modelos de madurez a nivel de ciberseguridad en las organizaciones, los cuales deben enfocarse en resolverse estar inquietudes frente a los diferentes panoramas de riesgo cibernético a nivel global y regional.

Inteligencia Cibernética usada para mitigar o evadir el impacto causado por las APT

Una de las causas antes comentadas, está relacionada con el impacto de estas amenazas y riesgos cibernéticos asociados, por ello, es vital facilitar los mecanismos necesarios para poder enfatizar los objetivos para cada una de las organizaciones, uno de estos, es el mejoramiento de las políticas que se poseen al interior de las organizaciones para poder contrarrestar estas amenazas. Por tal motivo es bueno identificar en que lugar se encuentra la ciberseguridad actualmente después de otro tipo de amenazas, como lo son, los extremos de lluvia, los cambios climáticos y los desastres naturales (WEB FORUM 2019); mediante el cual poder revisar la importancia que actualmente existe para medir estos acercamientos, desde una una postura de “anticipación” ante estos fenómenos:

[7] El exploit EternalBlue había sido anteriormente identificado, y Microsoft emitió parches en marzo de 2017 para acabar con el exploit en las versiones de Windows Vista, Windows 7, Windows 8.1, Windows 10, Windows Server 2008, Windows Server 2012, y Windows Server 2016. No obstante, el ataque WannaCry infectó muchos sistemas que todavía usaban antiguos sistemas operativos Windows o versiones tempranas de los sistemas operativos más nuevos que todavía poseían el exploit, o aquellos en los que los usuarios no habían seguido los pasos apropiados para descargar el parche. Microsoft emitió nuevos parches para Windows XP y Windows Server 2003 así como versiones anteriores de los otros sistemas operativos el día siguiente al ataque del WannaCry. Lesley Carhart, experto de seguridad, declaró que "cada método de explotación que el ataque utilizó para propagarse podía haberse prevenido con la documentación adecuada

CIBERSEGURIDAD: METODOLOGÍA APROXIMADA PARA REALIZAR INVESTIGACIÓN EN INTELIGENCIA CIBERNÉTICA



Recuperado del Foro Económico Mundial – Informe Davos Suiza

Durante la actual pandemia covid19, la inteligencia cobra un gran valor argumentativo ante esta fehaciente necesidad, de tal manera, uno de los fundamentos radica en el componente de la evaluación de los riesgos asociados, así:

Figura elaborada por el autor para ilustrar los riesgos asociados

CIBERSEGURIDAD: METODOLOGÍA APROXIMADA PARA REALIZAR INVESTIGACIÓN EN INTELIGENCIA CIBERNÉTICA

En virtud de lo anterior se observa que cada uno de los factores que se identifican ante una acción y decisión tomada en el país u organización posee unos riesgos debidamente asociados que permiten que las amenazas se puedan desarrollar o materializar, por ende, es importante dentro del análisis de contexto de la amenaza, establecer su posible impacto, como lo sucedido en Ucrania con WannaCry.

En la anterior figura (Foro económico mundial) se evidencia el nivel de importancia de los ciberataques son los aspectos que pueden impactar una nación y una realidad a nivel de la industria y el impacto sobre las organizaciones, por eso es importante determinar aspectos que realmente están enfocadas hacia los elementos fundamentales (impacto y la probabilidad) hacia las necesidades fundamentales para poder actuar ante estas consecuencias y sus principales rasgos hacia el "*core bussiness*" y el aspecto de recuperabilidad.

Asimismo, estos escenarios se involucran ante las necesidades de la organización y los enfoques que puedan obtener citada información con los principales aspectos que se derivan la información interna y externa que se visibilice ante las diferentes partes interesadas.

La producción de datos realizada por medio de las fuentes de información se debe obtener por medio de diferentes fuentes asociadas a diferentes esquemas internos que poseen los atributos necesarios para poder clasificar y categorizar esta información.

De otra manera es vital comprender en tres vías fundamentales que se describen (Future, 2019) en tres aspectos:

- *Los equipos de operaciones de seguridad son rutinariamente incapaces para procesar el flujo abrumador de alertas que reciben.*

- *La inteligencia de amenazas se puede integrar con las soluciones de seguridad que ya usan, ayudándoles priorizar y filtrar automáticamente alertas y otras amenazas; Los equipos de gestión de vulnerabilidades deben, Priorizar con precisión las vulnerabilidades más importantes.*

- *La inteligencia de amenazas proporciona acceso a ideas y contexto que los ayuda a diferenciar amenazas inmediatas a su empresa específica de simplemente amenazas potenciales.*

CIBERSEGURIDAD: METODOLOGÍA APROXIMADA PARA REALIZAR INVESTIGACIÓN EN INTELIGENCIA CIBERNÉTICA

- *Prevención de fraude, análisis de riesgos y otros. El personal de seguridad de alto nivel tiene el desafío de comprender el panorama actual de amenazas.*

- *Inteligencia de amenazas proporciona información clave sobre los actores de amenazas, sus intenciones y objetivos, y sus tácticas, técnicas, y procedimientos (TTP).*

Mediante estos aspectos de pueden redefinir los intereses de la organización en conocer cual es dinámica actual para poder enfrente las siguientes amenazas emergentes que de ejecutan en diferentes escenarios en los que deseen actuar las organizaciones a nivel de inteligencia.

Como se refleja en los aspectos anteriores, el enfoque de inteligencia busca siempre establecer los elementos relevantes o accionables para poder dinamizar el flujo de mitigación y anticipación de los riesgos y amenazas cibernéticas. De tal modo que esta información le permita enfocar cada una de las consecuencias adecuadas para su administración.

Este ciclo de información posee unos atributos internos y externos, los cuales debe poseer una finalidad específica y que sea realmente de provecho técnico, estratégico y operativo para la organización o país.

ESPACIO EN BLANCO

CIBERSEGURIDAD: METODOLOGÍA APROXIMADA PARA REALIZAR INVESTIGACIÓN EN INTELIGENCIA CIBERNÉTICA

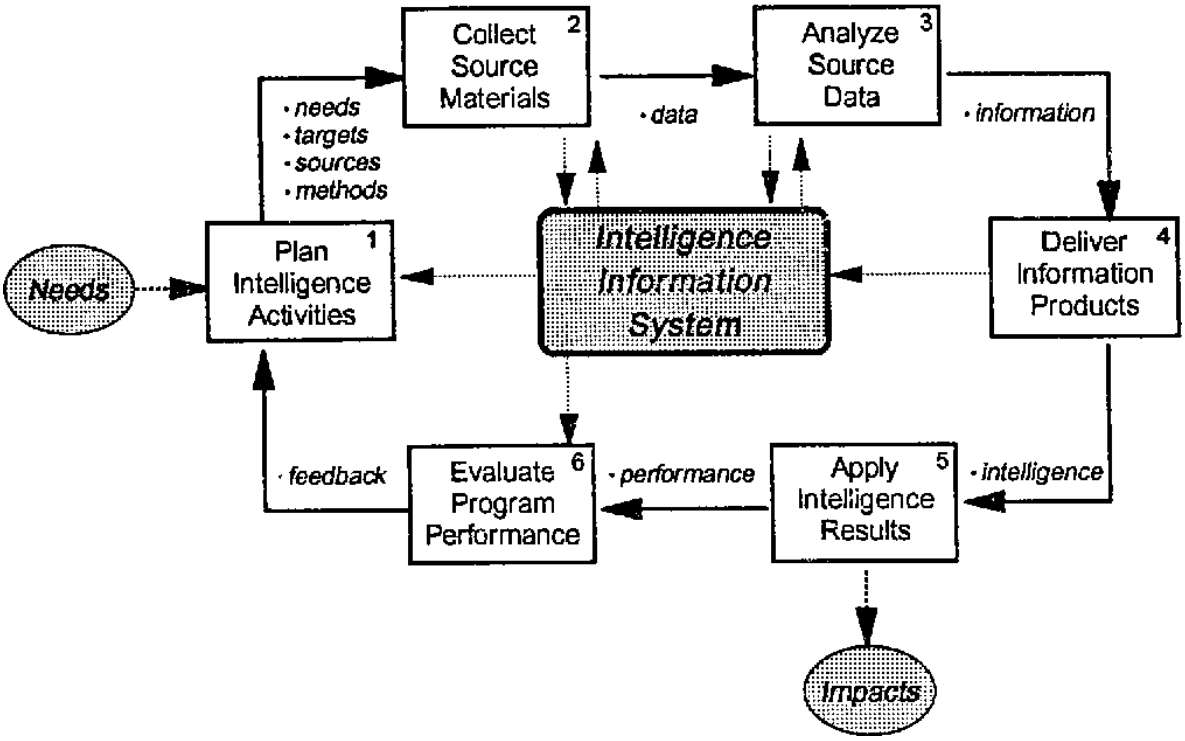


Figura tomada del paper Technical intelligence in business: understanding technology threats and opportunities (W. Bradford Ashton, 2014)

Esas necesidades parten para crear un *plan de inteligencia y unas actividades, en donde se requiera obtener esas determinadas fuentes, origen de los datos, generación de unos productos para aplicar determinadas estrategias para mitigar el posible impacto que puede ocasionar la amenaza*, Ej: APT.

Posteriormente determinar las fuentes de esta información requiere determinar si se poseen a nivel interior de la organización, un SOC (Security Operation Center) NO (Network Operation Center) o SIEM[8] (System Information Event Managment). De la misma manera si se posee un equipo de mitigación, remediación, un equipo de gestión y respuesta a incidentes, equipo de Cyber Treath Intelligence (CTI) o equipo de seguridad y/o ciberseguridad.

[8] Un sistema de **gestión de información y eventos de seguridad** (en inglés, *security information and event management*, SIEM) es un sistema que centraliza el almacenamiento y la interpretación de los datos relevante de seguridad. De esta forma, permite un análisis de la situación en múltiples ubicaciones desde un punto de vista unificado que facilita la detección de tendencias y patrones no habituales. La mayoría de los sistemas SIEM funcionan desplegando múltiples agentes de recopilación que recopilan eventos relacionados con la seguridad

CIBERSEGURIDAD: METODOLOGÍA APROXIMADA PARA REALIZAR INVESTIGACIÓN EN INTELIGENCIA CIBERNÉTICA

De mismo modo es importante determinar el origen y los atributos de la información a recolectar, empezando por definir la información accionable que permite tomar decisiones frente a una amenaza en particular, la cual podría estar relacionada de la siguiente manera:

- **Identificación por herramientas de seguridad:** Son todas aquellas relacionadas con las herramientas perimetrales, antivirus o de detección que posee la organización, a partir de los diferentes correlacionados entre sí.

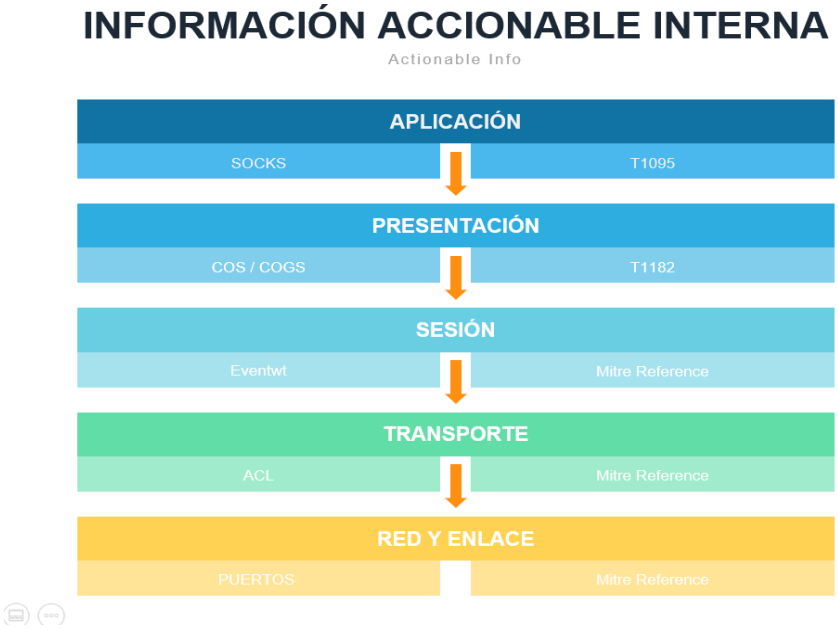


Figura elaborada con el fin de ilustrar la información interna de inteligencia

- **Identificación de fuentes externas o inteligencia de distintas fuentes:** Todas aquellas determinadas en Darkweb[9] o fuentes OSINT[10].

[9] La ***dark web*** o **internet oscura** es el contenido de la World Wide Web[1] que existe en *darknets*, redes que se superponen a la internet pública y requieren de software específico y configuraciones o autorización para acceder. Forma parte de la internet profunda, la parte de la web no indexada por los motores de búsqueda.[2345] Las *darknets* que constituyen la *dark web* incluyen pequeñas redes amigo-a-amigo P2P, así como grandes redes populares como Freenet, I2P, y Tor, operadas por organizaciones públicas y particulares. Los usuarios de la *dark web* usan el término *Clearnet* para hablar de la Internet no oscura, debido a su naturaleza sin cifrar

[10] **Inteligencia de fuentes abierta** (**OSINT**) son datos recogidos de fuentes disponibles de forma pública para ser utilizados en un contexto de inteligencia. En la comunidad de inteligencia, el término "abiertas" se refiere a fuentes disponibles públicamente (en el sentido de opuestas a fuentes secretas o clandestinas). No está relacionado con software libre o software de fuentes abiertas o inteligencia colectiva.

CIBERSEGURIDAD: METODOLOGÍA APROXIMADA PARA REALIZAR INVESTIGACIÓN EN INTELIGENCIA CIBERNÉTICA

Estas cinco capas son las establecidas para poder enfocar la obtención de la información con relación a los diferentes medios de captura existentes en el mercado: Aplicación, Presentación, Sesión, Transporte, Red y Enlace.

Del mismo modo, poder relacionar cada uno de estos eventos dirigidas en transmisión a través de las herramientas de seguridad establecidas, a la que se denomina **información accionable interna.**

Un principal escenario es poder determinar algunos aspectos destacados dentro de las entradas obtenidas, con el fin de generar datos que permitan establecer realmente "información accionable" y permita crear actividades que faciliten la toma de decisiones.

En ciberseguridad se vuelven relevantes los tipos de datos que se obtienen por medio de IP´s las cuales nos generan información asociada a un servicio en internet utilizando determinados protocolos de transporte (TCPIP[11]), Url´s , [12]hashes, las cuales se vuelven relevantes cuando se toman acciones técnicas frente a la defensa de estos dispositivos perimetrales o de detección. Sin embargo, este proceso de inteligencia sobre estos datos debe poseer un ciclo respectivo para poder determinar realmente cuales son estas decisiones, tácticas, estratégicas u operativas.

El ambiente o ecosistema de seguridad en la organización deberá comprender cuáles son sus fuentes, asimismo su impacto relacionado con esta obtención; a partir de ello, definir los niveles de esa información, y el uso final para su correlación y actividad de inteligencia productiva.

Lo primero a tener en cuenta previamente a evaluar esta información y sus métodos de entrada, es establecer quienes, y cuáles pueden ser los actores de las amenazas, adversarios frente a la organización y los riesgos asociados a estos elementos fundamentales para poder facilitar la finalidad determinada. En esta fase, se determinan si la información colectable es importante para suministrar la información a las tres variables (*Táctica, Técnica y Operativa*).

---

[11] M**odelo TCP/IP** es una descripción de protocolos de red desarrollado por Vinton Cerf y Robert E. Kahn, en la década de 1970. Fue implantado en la red ARPANET, la primera red de área amplia (WAN), desarrollada por encargo de DARPA, una agencia del Departamento de Defensa de los Estados Unidos, y predecesora de Internet; por esta razón, a veces también se le llama **modelo DoD** o **modelo DARPA**.

[12] **Hash:** Calculo algorítmico o procedimiento matemático que refleja el contenido, metadatos y originalidad de un dato o información.

CIBERSEGURIDAD: METODOLOGÍA APROXIMADA PARA REALIZAR INVESTIGACIÓN EN INTELIGENCIA CIBERNÉTICA

Figura elaborada por el autor con el fin establecer los tres factores de interés para la organización

El mejoramiento del "*profit*" de inteligencia cibernética se basa en tres aspectos esenciales requieren de una persona que ilustre los tipos de preguntas a solucionar frente a esos riesgos cibernéticos, y para ello es importante delimitar el alcance de las tres finalidades: Estratégico, Táctico y Operacional.

Los tres aspectos enunciados, permiten ser transversales a nivel de cumplimiento ante la normatividad de ISO 27001, ISO 27032, FrameWork de Ciberseguridad de NIST, implementación de estándares como, COSO, COBIT, Magerit y Octave. Por ende, las decisiones que se tomen ante las amenazas cibernéticas pueden enfocarse según la necesidad, contexto y ámbito de la organización.

Con el fin de elaborar, y colocar esos atributos que pueden presentarse frente a estos tres aspectos fundamentales se deben asociar a tres nuevos aspectos que pueden dilucidar otro tipo de datos de mayor complejidad, como lo son; las tácticas, técnicas y procedimientos o llamadas TTP, las cuales son definidas por (MITRE, 2010) de la siguiente manera:

CIBERSEGURIDAD: METODOLOGÍA APROXIMADA PARA REALIZAR INVESTIGACIÓN EN INTELIGENCIA CIBERNÉTICA

Las tácticas representan el "por qué" de una técnica ATT & CK.

Es el objetivo táctico del adversario: *la razón para realizar una acción. Las tácticas sirven como categorías contextuales útiles para técnicas individuales y cubren las anotaciones estándar de las cosas que los adversarios hacen durante una operación, como persistir, descubrir información, moverse lateralmente, ejecutar archivos y filtrar datos. Las tácticas se tratan como "etiquetas" dentro de ATT & CK donde una técnica está asociada o etiquetada con una o más categorías de tácticas dependiendo de los diferentes resultados que se pueden lograr mediante el uso de una técnica. Cada táctica contiene una definición que describe la categoría y sirve como guía para qué técnicas debería estar dentro de la táctica. Por ejemplo, la ejecución se define como una táctica que representa técnicas que resultan en la ejecución de código controlado por el adversario en un sistema local o remoto. Esta táctica a menudo se usa junto con el acceso inicial como medio para ejecutar el código una vez que se obtiene el acceso, y el movimiento lateral para expandir el acceso a sistemas remotos en una red. Se pueden definir categorías de tácticas adicionales según sea necesario para describir con mayor precisión los objetivos adversarios. Las aplicaciones de la metodología de modelado ATT & CK para otros dominios pueden requerir categorías nuevas o diferentes para asociar técnicas, aunque puede haber cierta superposición con las definiciones tácticas en los modelos existentes.*

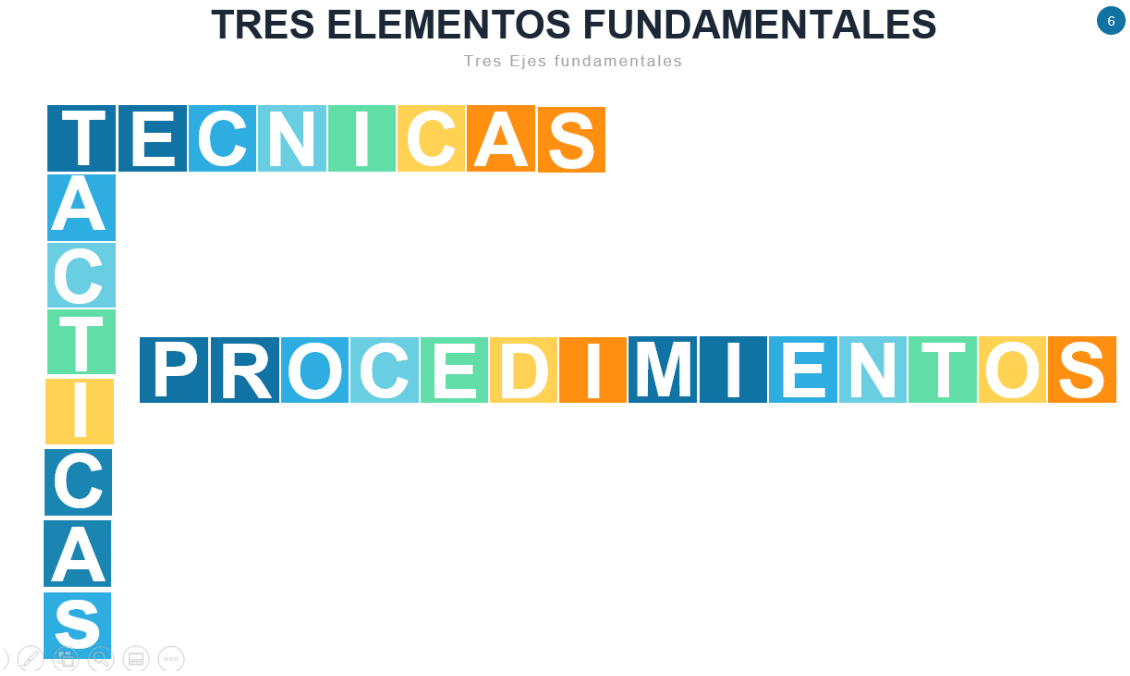


Figura elaborada por el autor para reforzar estos argumentos

CIBERSEGURIDAD: METODOLOGÍA APROXIMADA PARA REALIZAR INVESTIGACIÓN EN INTELIGENCIA CIBERNÉTICA

Técnicas representa "cómo" *un adversario logra un objetivo táctico al realizar una acción. Por ejemplo, un adversario puede volcar las credenciales para obtener acceso a credenciales útiles dentro de una red. Las técnicas también pueden representar "qué" gana un adversario al realizar una acción. Esta es una distinción útil para la táctica Discovery ya que las técnicas resaltan qué tipo de información busca un adversario con una acción en particular. Puede haber muchas formas o técnicas para lograr objetivos tácticos, por lo que hay múltiples técnicas en cada categoría de táctica.*

Procedimiento: *La manera de ejecutar las distintas técnicas y tácticas enfocadas en la victima expuesta o hiperconectada se pueden ejecutar y pueden casuar el impacto relacionado en un riesgo cibernético en específico.*

Así como lo evidencia MITRE, cada una de las tácticas, técnicas y procedimientos posee una estructura mediante la cual van enfocadas las necesidades estratégicas, tácticas y operacionales de una organización, y poder delimitar su "*profit*" esencial de inteligencia de amenazas e inteligencia cibernética.

Otro aspecto importante a tener en cuenta en la elaboración de esta metodología para aproximarse al recaudo y obtención de datos que permitan asignar valor a todas las fuentes de entrada relacionada tiene que ver con lo relacionado al rol que desempeña las fuentes OSINT; y sobre ello es vital comprender los principales estudios que argumentan como fuente de información de validez dirigida a ese escenario. La finalidad de permitir como punto de entrada de información accionable a la darkweb o web oscura, la cual permite determinar valores orientados a los mecanismos del crimen como servicio o cibercrimen localizado en esas fuentes.

De tal manera, también es necesario desarrollar a nivel interno establecer cuáles serían los enfoques estructurales de análisis a tener en cuenta; por ello la necesidad de orientar los puntos relativos a correlacionar. Sobre esto existen algunos estudios que se dirigen a tomar medidas de confiabilidad y de certeza sobre la información misma, algunos de estos aspectos están enfocados en la denominada pirámide del dolor, citada por varios autores sobre la dinámica activa de las entradas de la información accionable:

CIBERSEGURIDAD: METODOLOGÍA APROXIMADA PARA REALIZAR INVESTIGACIÓN EN INTELIGENCIA CIBERNÉTICA

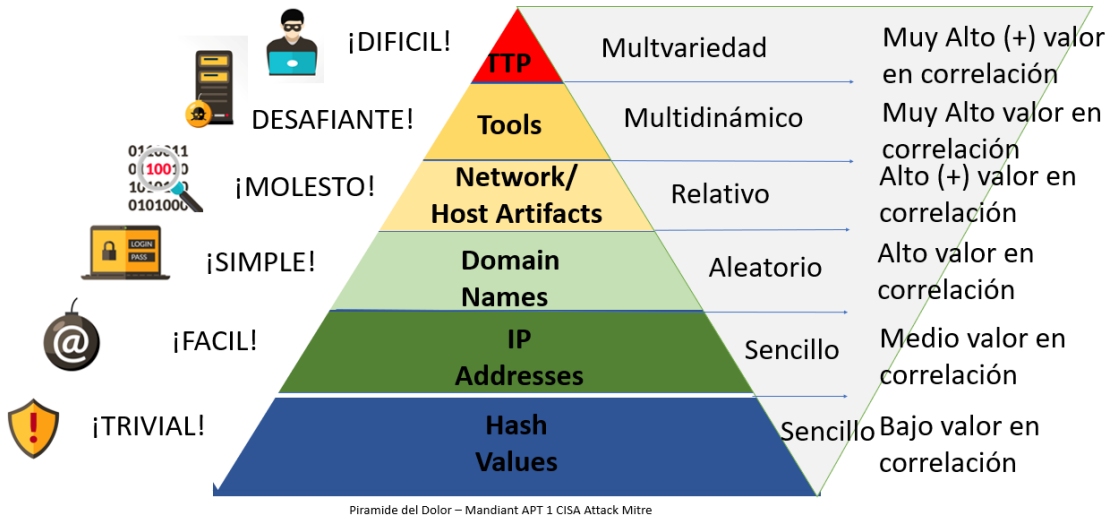


Figura elaborada por el autor para diagramar los aspectos a tener en cuenta en el análisis de fuentes

Esta pirámide del dolor se refiere a seis aspectos a tener en cuenta:

- **Los valores Hash:** Están orientados a la comparación o relacionamiento de valores hash, la cual se orienta al cálculo algorítmico de un evento de seguridad o Indicador de Compromiso.
- **Direcciones IP:** Están asociadas a la dirección única que representa un servicio, servidor o host dentro de una red.
- **Nombres de dominio:** Es la identificación única en internet de ese servicio, fácilmente ubicada por medio de la dirección IP.
- **Artefactos de red:** Son todos aquellos elementos obtenidos de la fuente información del modelo OSI[13].
  Herramientas, y
- **Tácticas técnicas y Procedimientos:** Lo relacionado al estándar de MITRE ATT@CK.

[13] El **modelo de interconexión de sistemas abiertos** (ISO/IEC 7498-1), más conocido como "modelo **OSI**", (en inglés, ***O**pen **S**ystem **I**nterconnection*) es un modelo de referencia para los protocolos de la red (no es una arquitectura de red), creado en el año 1980 por la Organización Internacional de Normalización (ISO).[1] Se ha publicado desde 1983 por la Unión Internacional de Telecomunicaciones (UIT) y, desde 1984, la Organización Internacional de Normalización (ISO) también lo publicó con estándar.[2] Su desarrollo comenzó en 1977

CIBERSEGURIDAD: METODOLOGÍA APROXIMADA PARA REALIZAR INVESTIGACIÓN EN INTELIGENCIA CIBERNÉTICA

Lo relacionado anteriormente, nos conduce a poder relacionar y entender, la estructura de conocimiento sobre la organización y sus amenazas cibernéticas, comprender la necesidad de formular preguntas basadas en estas fuentes de información accionable, redefinir aquellos aspectos que la ciberseguridad requiere para poder enfocar sus esfuerzos en análisis, y sobre todo, en relativizar los componentes que trae consigo determinar sus su comando y control táctico y operativo, así:

Figura elaborada para definir los controles (CCT)

EL Comando y Control Táctico deberá poseer la capacidad de identificar y resaltar los eventos de seguridad destacados con un adecuado filtro de importancia, además de poder detectar los rangos de acción por medio de las herramientas de seguridad: *Intrusion Detection System IDS, Intrusion Prevention System IPS o SIEM*. Lo cual permitirá activar preventivamente acciones, per o además, poder documentar y desarrollar un plan para poder tomar decisiones eficientes para el desarrollo de próximas defensas.

En segunda opción, también poseer un Comando y Control Operativo como se refleja en la siguiente gráfica:

CIBERSEGURIDAD: METODOLOGÍA APROXIMADA PARA REALIZAR INVESTIGACIÓN EN INTELIGENCIA CIBERNÉTICA

Figura elaborada en la aplicabilidad de inteligencia de amenazas de manera operacional

El comando y control operativo u operacional permitirá enfocar las entradas de información accionable interna y externa, así como crear la gestión documental de la información recolectada para su procesamiento, y ciclo de inteligencia cibernética. A partir de estos dos comandos se pueden enfocar la construcción de los indicadores de análisis operacional de inteligencia de amenazas y solucionar los tres factores principales de la organización.

Posteriormente se pueden construir los tableros para la generación de inteligencia aplicada y de inteligencia operacional. Del mismo modo poder enfatizar en los posibles escenarios de riesgos cibernéticos que posea la organización con la creación de metodologías *Red Team y BlueTeam* analizados por (Ortiz Ruiz , Metodologia para la simulación de ataques cibernéticos adversariales, 2020) en el momento de generar conocimiento de defensa y de proactividad frente a la ciberseguridad.

Modelos de entrenamiento para desarrollar datos mediante indicadores:

Una vez se establecen los cuadros de mando y control (operacional y táctico) se procede a levantar los datos necesarios mediante la información accionable, interna y externa de la organización basado en sus potenciales amenazas. Con esta información se procede a revisar los indicadores que

contendrán la información necesaria para poder evaluar la proximidad, el compromiso x impacto y compromiso por criticidad, así:

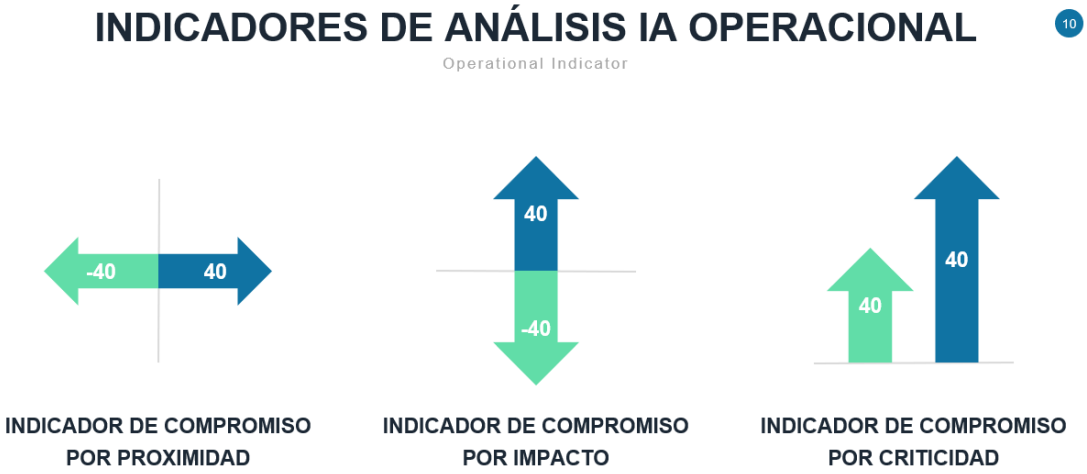


Figura elaborada de los indicadores de inteligencia de amenazas cibernéticas

Con base a estos indicadores se puede de manera paralela, elaborar los indicadores de inteligencia de amenazas táctica, el cual desarrollará los aspectos de: indicadores de compromiso por credibilidad, indicador de compromiso por incertidumbre e indicadores de compromiso por falencia.

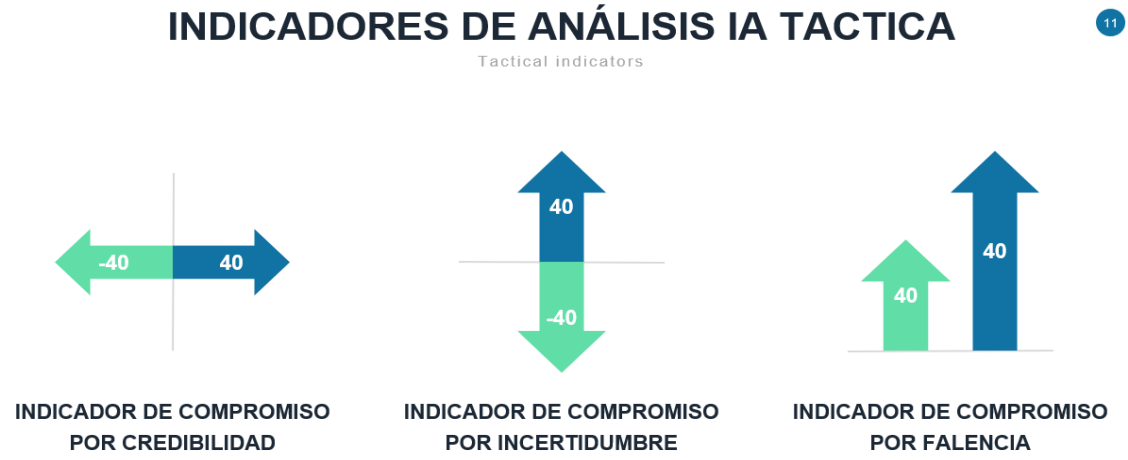


Figura elaborada por el autor para esquematizar los indicadores de amenaza táctica

Posteriormente se pueden elaborar los indicadores de análisis de inteligencia de amenazas en lo estratégico, lo permitirá ajustarse a las necesidades de la economía actual, los retos y la visión de la organización en materia de ciberseguridad.

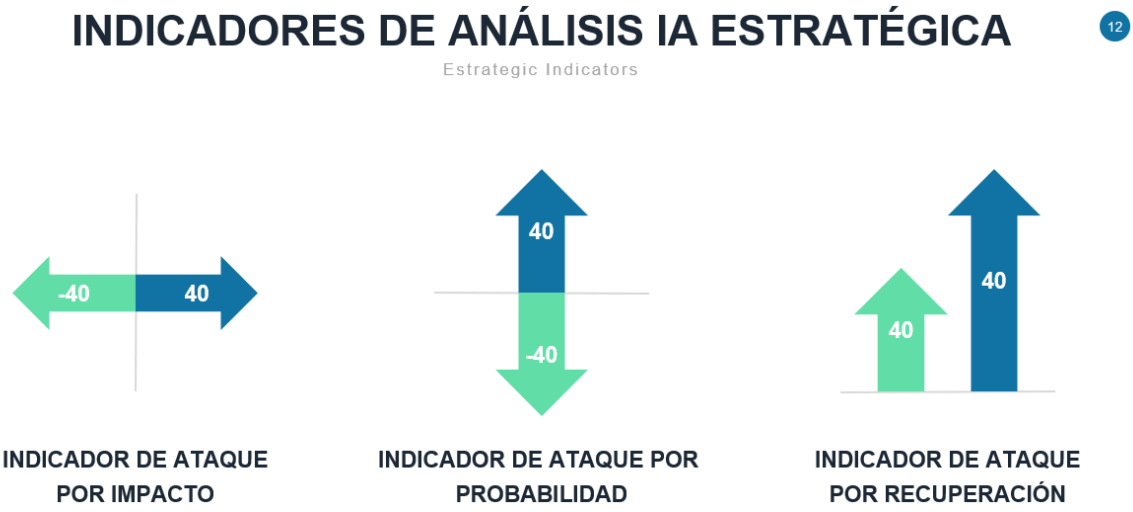


Figura elaborada por el autor para ilustrar el análisis de inteligencia de amenazas a nivel estratégico

La evaluación de los indicadores de ataque por impacto, ataque por probabilidad y ataque por recuperación, permite trazar la proyección a futuro de la organización; con ello se permite elaborar y modificar el mapa de riesgos cibernéticos que poseía la organización o que puede implementarse a futuro.

Para ello, es importante definir la primera entrada de información relacionada con las herramientas de seguridad. En este sentido poder delimitar el modelo de identificación de estas entradas para facilitar su correlación existente, así:

CIBERSEGURIDAD: METODOLOGÍA APROXIMADA PARA REALIZAR INVESTIGACIÓN EN INTELIGENCIA CIBERNÉTICA

Figura elaborada para ilustrar el diagrama de fuentes de información

Este esquema permite conectar los nodos de interacción por medio de alguna herramienta que facilite la interoperabilidad, y poder estandarizar y contabilizar los datos obtenidos; por medio de detección de curvas tempranas y detecciones de anomalías extendidas por medio de sus atributos.

Respectivamente, estos enfoques deben ser testeados y revisados para que se orienten según las necesidades o preguntas estratégicas formuladas; con el fin de reorientar los esquemas actuales de seguridad expuestos.

CIBERSEGURIDAD: METODOLOGÍA APROXIMADA PARA REALIZAR INVESTIGACIÓN EN INTELIGENCIA CIBERNÉTICA

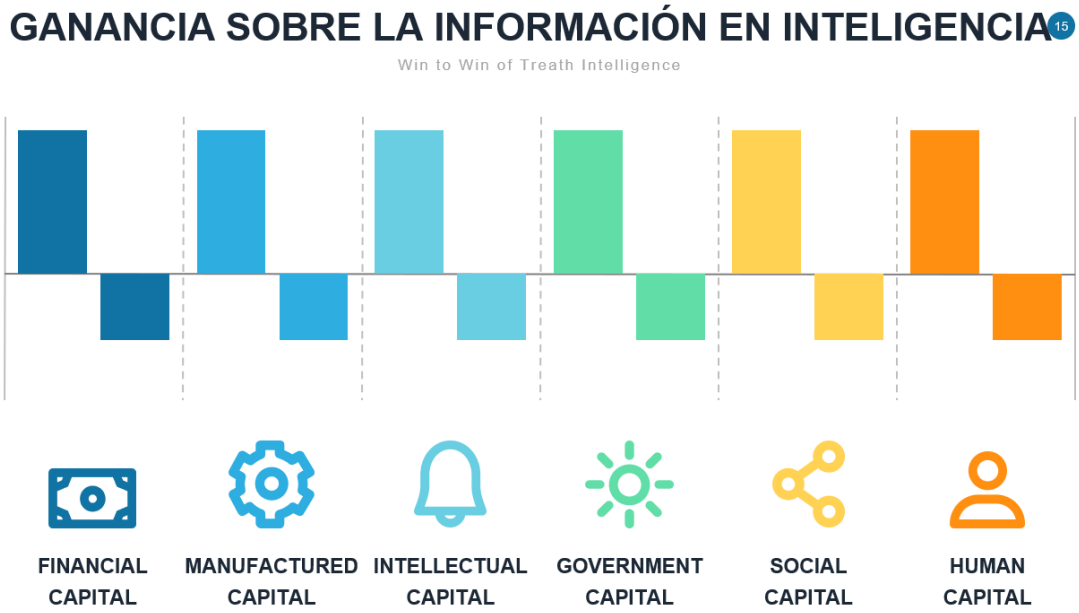


Figura elaborada para ilustrar los beneficios de la metodología

Estos argumentos antes enunciados, son orientadores, y permiten redefinir las políticas de seguridad en la información, seguridad informática y ciberseguridad de empresas y organizaciones, los cuales desconocen realmente quienes pueden afectar su economía y negocio; aquellas que, por el simple hecho de competir, no poseen las capacidades necesarias para poder procesar, analizar y proyectar su visión en adquisiciones tecnológicas o de transformación digital. A partir de esto, se puede elaborar un esquema ajustado y necesario para poder fortalecer cada una de las actividades de los grupos de trabajo, mesas técnicas y equipos de seguridad.

La metodología ofrece elementos tangibles para poder encaminar aspectos de interés y desarrollo estratégico a nivel de compañía u organización; de la misma manera que orienten a las diferentes partes interesadas, proveedores críticos o en riesgo, cadenas de suministro o vendedores.

Este artículo también tiene como finalidad sentar las bases de estado del arte en la materia de inteligencia cibernética, la cual propone varios escenarios transversales en función de la ciberseguridad y el marco de trabajo del Instituto Nacional de Estándares en Tecnología NIST.

CIBERSEGURIDAD: METODOLOGÍA APROXIMADA PARA REALIZAR INVESTIGACIÓN EN INTELIGENCIA CIBERNÉTICA

Del mismo modo en apoyo o fomento del crecimiento en los equipos de seguridad cibernética y de inteligencia cibernética para las organizaciones y demás áreas de apoyo en la cual se administren o se de tratamiento adecuado a los riesgos cibernéticos. Considerando en este mismo sentido que, las amenazas cibernéticas como lo demostró actualmente la pandemia cibercovid19, no permite dar espera a las vinculaciones o necesidades en ciberseguridad que exige la industria, y que, por lo tanto, es vital tomar conciencia y despertar del letargo que muchas organizaciones actualmente poseen en ciberseguridad.

En la próxima realización o segunda parte de este artículo se podrá estructurar un caso de uso frente a la temática planteada, permitiendo con esta, afianzar debidamente los conceptos y poder familiarizar una Amenaza Avanzada Persistente con los atributos que ella misma posee.

CIBERSEGURIDAD: METODOLOGÍA APROXIMADA PARA REALIZAR INVESTIGACIÓN EN INTELIGENCIA CIBERNÉTICA

BIBLIOGRAFIA

Cybersecurity, N. (2018). NIST Cybersecurity Framework.

EC3, I. (2019). *Internet Organised Crime Threat Assessment (IOCTA).* The Hague: European Union Agency for Law Enforcement Cooperation 2019.

FIRST. (s.f.). *https://www.first.org/about/*. Obtenido de https://www.first.org/about/: https://www.first.org/about/

Framework, I. S., & Security, I. (2020). *http://www.alntechnology.com/sites/default/files/isfpdf%20%28rombus%29.pdf.* Obtenido de http://www.alntechnology.com/sites/default/files/isfpdf%20%28rombus%29.pdf: http://www.alntechnology.com/sites/default/files/isfpdf%20%28rombus%29.pdf

Future, R. (2019). *The Treath Intelligence Treath Book.*

ICONTEC. (s.f.). ISO . *DIRECTRICES ISO 27001*.

Instituto Nacional, E. E. (21 de 04 de 2020). Obtenido de Framework for Improving Critical Infrastructure Cybersecurity

ISACA. (2013). *Amenazas persistentes avanzadas, Cómo gestionar el riesgo para su engocio.* Reino Unido: ISACA.

ISO, 2. I. (2014). Guidelines for identification, collection, acquisition and preservation of digital evidence" ISO/IEC 27037:2012.

Mellon, C. U. (Junio de 1999). *https://resources.sei.cmu.edu/.* Obtenido de https://resources.sei.cmu.edu/asset_files/: https://resources.sei.cmu.edu/asset_files/TechnicalReport/1999_005_001_16769.pdf

CIBERSEGURIDAD: METODOLOGÍA APROXIMADA PARA REALIZAR INVESTIGACIÓN EN INTELIGENCIA CIBERNÉTICA

MITRE. (2010). *https://stids.c4i.gmu.edu/STIDS2010/presentations/STIDS_talk_A8_Parmelee.pdf.* Obtenido de https://stids.c4i.gmu.edu: https://stids.c4i.gmu.edu/STIDS2010/presentations/STIDS_talk_A8_Parmelee.pdf

MITRE, C. (s.f.). Malware . *Captalogación del Malware*.

Moira J. , W.-B., Don , S., & Klaus, P. (2003). *Handbook for Computer Security Incident Repsonse .* National Science Foundation.

NIST, S., & SP 800 61. (s.f.). *https://www.csirt.org/publications/.* Obtenido de CSIRT: https://www.csirt.org/publications/sp800-61.pdf

OEA, S. C. (s.f.). *www.oas.org.* Obtenido de www.oas.org › spanish › Convención de Palermo _ESP

Ortiz Ruiz , E. E. (Mayo de 2020). Metodologia para la simulación de ataques cibernéticos adversariales.

Ortiz Ruiz, E. E. (Agosto de 2018). Blockchain: Conceptos básicos aplicables para reducir la brecha del Fraude. *Blockchain: Conceptos básicos aplicables para reducir la brecha del Fraude*.

Ortiz Ruiz, E. E. (2019). Evidencia Digital: Fundamentos aplicables para el abordaje de la Examinación. *Evidencia Digital: Fundamentos aplicables para el abordaje de la Examinación*.

Ortiz Ruiz, E. E. (02 de Abril de 2019). Evidencia Digital: Principios metodológicos para el análisis de Código Malicioso. *Evidencia Digital: Principios metodológicos para el análisis de Código Malicioso*. Bogotá: ResearchGate.

Ortiz Ruiz, E. E. (2020). LIBRO SOBRE A APLICAO PRACTICA DA INVESTIGACAO CRIMINAL TECNOLOGICA. En Coautores. Brasil: Juspodivm.

Ortiz, E. E. (2020). APROXIMACIÓN METODOLÓGICA DEL CIBERCRIMEN EN COLOMBIA. *Seguridad*, 20.

Penedo, D. (2005). Technical Infraestructure of a CSIRT.

RFC 2196, B. (1997). *Site Security handbook.* IETF.

Rohmeyer , p., & Bayuk , J. (2019). *Financial Cybersecurity Risk Manangement.* Hoboken NJ, USA: Springer. Recuperado el 17 de Marzo de 2020

Sultan , A., & Majeed , A. (2014). *Information Security Maturity Model For NIST CSF.* Arabia Saudita: College of Computer Sciences and Engineering. Obtenido de

CIBERSEGURIDAD: METODOLOGÍA APROXIMADA PARA REALIZAR INVESTIGACIÓN EN INTELIGENCIA CIBERNÉTICA

https://s3.amazonaws.com/academia.edu.documents/52007982/csit76505.pdf?response-content-disposition=inline%3B%20filename%3DINFORMATION_SECURITY_MATURITY_MODEL_FOR.pdf&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWOWYYGZ2Y53UL3A%2F20200317%2Fus-e

Toro, M. M., Ortiz, E. E., & Parada, W. (2018). *Fundamentos de la investigación forense en ambientes informáticos.*

W. Bradford Ashton, G. S. (2014). *Technical intelligence in business: understanding technology threats and opportunities.*

Wikipedia. (21 de 04 de 2020). *https://es.wikipedia.org/wiki/Ciberataques_en_Ucrania_de_2017*. Obtenido de https://es.wikipedia.org/wiki/Ciberataques_en_Ucrania_de_2017