Amenazas Compartidas - AmeComp

Edgar Yesid Garay Medina

Trabajo de grado para optar al título profesional:

Maestría en Ciberseguridad y Ciberdefensa

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia

2018

MINISTERIO DE DEFENSA NACIONAL

COMANDO GENERAL FUERZAS MILITARES

ESCUELA SUPERIOR DE GUERRA

"General Rafael Reyes Prieto"
Unión, Proyección, Liderazgo

AMENAZAS COMPARTIDAS

AMECOMP

ALUMNO: EDGAR YESID GARAY MEDINA

DIRECTOR: STEVEN JONES CHALJUB

MAESTRIA EN CIBERSEGURIDAD Y CIBERDEFENSA

TRABAJO DE GRADO PARA OPTAR EL TITULO DE MAGISTER EN CIBERSEGURIDAD Y CIBERDEFENSA

BOGOTA – COLOMBIA

2018

Ministerio de Defensa Nacional
Comando General de las Fuerzas Militares
Escuela Superior de Guerra
Maestría en Ciberseguridad y Ciberdefensa

"General Rafael Reyes Prieto"
Unión, Proyección, Liderazgo

Amenazas Compartidas - AmeComp

Edgar Yesid Garay Medina

Director
Steven Jones

Investigación Estratégica

Maestría en Ciberseguridad y Ciberdefensa
Trabajo de grado
Bogotá – Colombia
2018

Página de aceptación del trabajo

Resumen

Este documento busca resolver la forma en que se podría mediante inteligencia de amenazas obtener datos reales y compartirlos sobre algún evento o incidente cibernético entre entidades miembro de una red de colaboración, enviando esta información a las entidades con características similares en su infraestructura tecnológica, minimizando los impactos y evitando afectar la reputación de la entidad emisora. Sobre el tema, se han desarrollado diferentes proyectos encaminados en la implementación de soluciones que permitan obtener información de eventos e incidentes cibernéticos ocurridos en entidades, mediante mecanismos de inteligencia de amenazas, permitiendo tomar acciones preventivas en otras entidades, al respecto y de gran importancia es que los datos reportados deben ser reales y aplicables a las entidades receptoras, sin tener la necesidad de conocer el origen del reporte, evitando afectar la reputación de alguna entidad por esta situación.

Abstract

This document seeks to identify ways in which, through intelligence and investigation into cyber threats, existing data related to cybersecurity breaches can be obtained and shared between members of a network, sending such information to institutions with a similar IT infrastructure in order to minimize the impact of the attack while avoiding potential damage to the reputation of the issuing entity.

Several different projects geared towards the implementation of solutions that make possible the acquisition of information, through intelligence gathered from analysis of cyber threats, have been developed, allowing preventative measures to be taken by other entities. In that regard, it is of great importance that the information reported is accurate and applicable to the receiving institution, without the requirement that the source of the report is known, thus mitigating potential damage to the reputation of the respective entities involved in the incident.

Palabras claves

Red de colaboración, indicadores de compromiso, amenazas cibernéticas, detección de incidentes, inteligencia de amenazas.

Key Word

Collaboration network, commitment indicators, cyber threats, Incident detection, threat intelligence.

Contenido

Contenido de Ilustraciones

Contenido de Tablas

Introducción

Actualmente existe para todas las organizaciones un avance generado por el uso de herramientas tecnológicas en sus procesos, con el propósito de facilitar y hacer eficiente el desarrollo de sus tareas según sus funciones o los servicios que presten, esto genera una dependencia de la tecnología. Esta tecnología puede estar en la entidad conectada a una red aislada o con alguna interface que permita sea vista desde internet facilitando su acceso y obtener información en tiempo real.

Los desarrollos tecnológicos de hoy en día creados por diferentes fabricantes, a pesar de involucrar procesos de calidad durante su construcción, tiene en su producto final diversas vulnerabilidades desconocidas por sus creadores, las cuales son descubiertas y aprovechadas en diversos casos por personas, organizaciones o gobiernos con la intención de afectar a la entidad que hace uso de esta tecnología mediante la alteración, interrupción o daño. Con el propósito de minimizar la materialización de estas amenazas, se han desarrollado diversas herramientas tecnológicas (herramientas de seguridad), para la protección ante diversos ataques, permitiendo incluso la detección y control en algunos de ellos; sin embargo, esto no descarta la posibilidad que el mismo ataque sea aplicado a otras entidades.

Varios fabricantes de herramientas de seguridad tienen desarrollos incorporados en sus tecnologías con el propósito de caracterizar archivos, direcciones de Internet, sitios web o tráfico de red involucrados en ataques, generando una especie de huella digital única (Indicador de

compromiso), para luego reportarla a sitios especializados en internet, encargados de replicar esta información a sus dispositivos en Internet evitando un posible contagio a otros clientes por ataques con estas características ya identificadas.

El presente documento se basa principalmente en el desarrollo de una guía que implementa elementos esenciales y pasos asociados con el objetivo de desarrollar el marco del proyecto ***AmeComp***, sobre el cual se dará respuesta a cómo crear un mecanismo, que mediante el uso de una red de colaboración de entidades, pueda reportar amenazas cibernéticas mediante indicadores de compromiso e inteligencia de amenazas de elementos involucrados en un ataque cibernético, sin depender de marcas exclusivas de dispositivos, en donde se retroalimenten a las entidades miembros de la red con características similares, sin el temor de que se afecte la imagen o reputación de quien reporta, y con la seguridad que los datos recibidos es real.

Para el desarrollo, se consideraron documentos publicados por Centro de Protección de Infraestructuras Nacionales (por sus siglas en ingles CPNI), siendo estos líderes del Reino Unido, en la definición de guías y políticas en seguridad, definiendo el desarrollo de los pasos para la recolección, el análisis, la producción, la evaluación y para compartir información en los niveles estratégicos, tácticos, operativos y técnicos en el ámbito ciber. La implementación de esta guía permite la implementación de un método propio, otros documentos se afianzan en el aumento de capacidades (Dalziel, 2015) o entidades como el Centro de Integración de Inteligencia en Ciber Amenazas (CTIIC) creado en el 2015.

El desarrollo de esta guía inicia desde la creación de grupos, identificando las etapas para el desarrollo de una colaboración, en este caso se define un solo grupo que corresponde al comité de Coordinación Seguridad del Sistema Financiero Colombiano, conformado por el Ministerio de Hacienda, el Banco de la Republica, la Super Intendencia Financiera y el Fondo de Garantías de Instituciones Financieras, sobre este grupo se identifican sus elementos en común basado en una toxemia definida.

Se deben definir actividades de contramedida en las diferentes líneas de la seguridad de las entidades, las cuales son el resultado del análisis de la información producto del uso de la red de colaboración, esta información sustentará decisiones en la estrategia de la entidad, al igual que en la parte operativa, táctica y técnica.

Una vez definidos los grupos de colaboración, la ganancia y el impacto de los resultados para cada entidad, se define la implementación de una herramienta que cumpla con las especificaciones necesarias para tener la información real y oportuna cumpliendo el propósito de realizar una preparación adecuada para evitar eventos sucedidos o contrarrestados en otras entidades.

Todo esto funciona siempre que se defina y se cumpla algunos lineamientos que deberán estar acorde a las entidades que conformarían la red que, dependiendo del tipo de entidad, generaría algunos convenios aceptados por los responsables de la seguridad en cada entidad.

La esencia de AmeComp, es desarrollar un mecanismos usado inicialmente por entidades del sector público, que permita mediante la suma de capacidades crear la unión mediante el intercambio de información de amenazas materializadas o que generaron algún efecto en una entidad; para esto se establece la creación de una red de colaboración entre entidades interesadas que aplicaran técnicas de inteligencia de amenazas como un producto de la información compartida, que genera una debida gestión de incidentes, de tal forma, que puedan compartir detalle de los elementos involucrados en los ataques mediante indicadores de compromiso, todo esto bajo unos lineamientos definidos y formalizados entre las partes que conforman la red de colaboración.

CAPÍTULO 1. ACERCAMIENTO SOBRE LOS COMPONENTES Y LA ACTUALIDAD PARA COMPARTIR AMENAZAS.

Red de Colaboración

Existen estudios documentados en Estados Unidos, que muestran la colaboración entre diversos sectores, siendo de valor tener acceso a esta información para poder crear un marco colaborativo para la creación del presente documento, tomando como base las etapas que permiten desarrollar una colaboración entre entidades, iniciando desde la filantropía que es parte de la cultura, posteriormente identificando eventos transaccionales e incluso integrativos, esto de acuerdo al estudio identificado en los aspectos claves de la colaboración (Romero et al., 2005). Las etapas son las siguientes:

Etapa filantrópica. Se trata del tipo más común respecto a las relaciones de colaboración entre las compañías, estas hacen referencia a las relaciones que se basan en donaciones que realiza una compañía, en respuesta a solicitudes por parte de otra. El nivel de compromiso y los recursos que se presentan son bajos, se presentan con escasa frecuencia, la gestión es muy sencilla y no contempla fines estratégicos, para este caso la organización posee una mentalidad benefactora y el receptor una actitud agradecida. Esta relación favorece a entidades que se pueden enmarcar dentro de una visión de la mayoría de las ONG. Para las empresas aportantes, este tipo de relación representan una manera de promover su imagen y desarrollar sus valores

como instituciones responsables y comprometidas. Esta etapa puede ser beneficiosa para algunas entidades.(Romero et al., 2005)

Etapa transaccional. En esta etapa las entidades tienen una mayor interacción con una tendencia en realizar actividades más específicas, donde se presentan un intercambio de valores, lo que indica que los beneficios se darían para ambas sin la necesidad que sean los mismos. Las organizaciones implementan sus capacidades y las relaciones pasan a ser relevantes dentro de la estrategia de cada entidad. En esta etapa se realizan actividades como programas de marketing de causas, auspicios de eventos, proyectos especiales y actividades de voluntariado de empleados. Esta etapa es la consecuente a la filantrópica (Romero et al., 2005)

Etapa integrativa. Es lo consecuente a la etapa transaccional, en donde están aquellas entidades que evolucionan hasta crear alianzas estratégicas, con misiones conjuntas, estrategias sincronizadas y valores compatibles. En este punto las entidades interactuar con mayor frecuencia y desarrollan una mayor cantidad y variedad de actividades en común. En esta etapa, el nivel de integración de las entidades corresponde más a un emprendimiento conjunto que a una simple transacción.(Romero et al., 2005)

Estas tres etapas no constituyen marcos excluyentes. La implementación de relaciones de colaboración implica tener presente riesgos y costos, otro elemento a considerar corresponde a que no es beneficioso para todas las empresas. No obstante, el mencionado estudio sobre colaboraciones realizado por el Banco Mundial concluye que "(...) el beneficio de las

asociaciones es muy grande... [y]... existe una creciente conciencia regional de dicho potencial... [Más aún,] se detecta una gran necesidad de asesoramiento sobre los mecanismos de creación de relaciones en los miembros de las asociaciones existentes y nuevas (...)" (Romero et al., 2005)

Compartir datos es una forma de generar de valor, lo cual es el estímulo que mantiene a las organizaciones activas y comprometidas. Se puede asumir que las colaboraciones tendrán un mayor potencial de generación de valor cuanto más hayan avanzado en el continuo. (Romero et al., 2005). Vivimos en un mundo con amenazas globales que son difíciles en atacar o retener de forma individual, lo que requiere la implementación de un frente de ataque colaborativo, compartiendo información para la realización de inteligencia.(Villalón, 2016).

Un elemento importante para el funcionamiento de la red de colaboración es el abandono de la búsqueda de poder por el conocimiento, para fundamentar así un espacio de conocimiento, lo que corresponde a un principio de inteligencia colectiva. (Trejo Medina, 2013)

El realizar una colaboración con un alto nivel de alineación entre las entidades participantes, generar un valor "a la medida" de las necesidades. Así mismo, el valor generado por estas colaboraciones será más difícil de imitar, puesto que resultará de las características únicas y distintivas de las organizaciones involucradas. (Romero et al., 2005)

Al desarrollar un tipo de colaboración que llegue a la estrategia de una organización, esta adquiere un alto nivel de importancia, generando incentivos mediante la asignación de recursos

con el propósito de crear compromisos. Esto se puede ver en diferentes ejemplos mencionados por el autor del libro. (Romero et al., 2005)

Amenazas Cibernéticas e Incidentes

La presencia en la Internet de cualquier organización, con el propósito de prestar algún servicio en el ciberespacio, crea la posibilidad que a través de este medio, se pueda generar una afectación que la perjudique, esta situación hoy día, es de conocimiento; por esta razón implementan algunos controles dificultando el aprovechamiento de sus vulnerabilidades, sin embargo, esto ha ocasionado que las amenazas cibernéticas maduren y sean sofisticadas evitando las defensas.(Andreeski et al., 2014)

Existen desarrollos de capacidades que buscan generar diferentes capas de seguridad, con el propósito de evitar o minimizar las amenazas cibernéticas, sin embargo, siempre es posible que en aquellos casos cuando los ataques son dirigidos y mantienen su persistencia (Andreeski et al., 2014), estos lleguen a cumplir su cometido dejando en la mayoría de las veces registro de lo sucedido permitiendo identificar y reconocer la forma en que se realizó el ataque cibernético (Galindo López, 2014). Estos ataques cibernéticos tienden a evolucionar, sobrepasando el propósito de los piratas informáticos maliciosos, al igual que aquellas personas que buscan la aplicación de códigos que buscan solo destruir la información de una web. (Andreeski et al., 2014)

Es fundamental el papel que tienen los proveedores de telecomunicaciones en el desarrollo de defensa cibernética proactiva y defensa en profundidad, debido a que, por sus funciones han desarrollado capacidades técnicas que permiten identificar el flujo del tráfico y ocasionalmente identifican intentos de afectaciones previas a que sucedan, ellos los hace parte de una solución dentro de los esquemas que se buscan implementar con el propósito de contrarrestar la amenazas en la red. (Andreeski et al., 2014). Otras fuentes de información importante son los Centros de Operaciones de Seguridad SOC por sus siglas en inglés, quienes proveen servicios de detección y reacción ante incidentes de seguridad, debido a sus funciones de monitoreo y administración de los aspectos de seguridad de la información de la organización en tiempo real.(Wong & González, 2008)

Las soluciones, tienden al desarrollo de arquitecturas de seguridad de próxima generación las cuales buscan disuadir, detectar y defender a la organización de sofisticadas amenazas. La implementación o desarrollo de una estrategia de defensa en profundidad que sea proactiva requiere necesariamente una capa de seguridad e inteligencia que se despliega en la organización, de esta forma se debe desarrollar la capacidad estratégica que detecta y mitiga los ataques evitando tráfico dañino dirigido a la organización o que salga de ella. El desarrollo de una estrategia debe ser enfocada a que sea proactiva de tal forma que aborde a la amenaza de forma previa y eficientemente. (Andreeski et al., 2014)

El desarrollo de herramientas que permiten detectar y manejar las amenazas cibernéticas tienden a tener una vida corta debido a la evolución de las amenazas que crean mecanismos o

métodos para evitarlos o saltarlos, lo que obliga a implementar soluciones que tienden a ser dinámicas y flexibles, permitiendo respuestas continuas y actualizadas para el control especialmente de aquellas amenazas conocidas como amenazas persistentes avanzadas (APTs) (Villalón, 2016), que son procesos orquestado por un tercero que puede ser un grupo delictivo, con la intención y capacidad de atacar de forma avanzada lo que incluye de diferentes formas y de manera continua en el tiempo un objetivo determinado, utilizadas usualmente contra gobiernos y grandes empresas con fines de espionaje. (Andreeski et al., 2014)

Cualquier tipo de organización sea pública o del sector privado debe enfrentar amenazas de seguridad cibernética creando desafíos, con variables como en el aumento en el volumen y la complejidad de los ataques dependiendo su atractivo para los atacantes. Esto exige la implementación de soluciones sofisticadas apuntando a la generación de defensa y que permita medir el progreso. Un modelo que pueda ser implementado debe desarrollar la capacidad en la organización que permita detectar, proteger, responder y recuperarse de incidentes cibernéticos. (Andreeski et al., 2014)

Se ha generado un aumento global en la materialización incidentes cibernéticos, creando un mayor grado de conciencia, con varios mecanismos que buscan prevenir que se presenten, gran parte de las estrategias se enfocan en la detección temprana y en el intercambio de información. En consecuencia, los espacios permitidos para que se realice un ataque cibernético es mucho menor, lo que ocasiona un aumento de habilidades por parte del atacante que incluso

ya ofrece servicios especializados pese a que es considerado como un delito cibernético. (Andreeski et al., 2014)

Es conveniente crear unidades especializadas y dedicadas para responder a incidentes de ciberseguridad, que apoyen a organizaciones de cualquier sector. El ejercicio realizado a nivel internacional al respecto a las actividades desarrolladas por estos equipos especializados conocidos como CERT (Computer Emergency Response Team) identifican como fortalece para hacer frente, la colaboración entre las organizaciones. (Andreeski et al., 2014)

Inteligencia de Amenazas

La inteligencia de amenazas es la información sobre la cual se puede realizar una acción, con el propósito de cambiar unos resultados. El tener información conocida o desconocida es relevante cuando se habla de inteligencia generado una amenaza o un riesgo respecto a algo que inicialmente no se sabe, pero existe, no se tiene datos respecto a ¿quién, por qué, cuándo o cómo?

Lo que se busca en la inteligencia de amenazas en convertir aquello desconocido en conocido, el poder descubrir la existencia de amenazas con el propósito de comprenderla para luego mitigarla antes de que el incidente se materialice. En general se busca poder reconocer la mayor cantidad de riesgos quedando en la categoría definida como "conocidos" y desarrollar varios que estén dentro de la categoría "desconocidas"; permitiendo que el menor número de

amenazas permanezca como "incógnitas desconocidas". Esto es un reto cuando se realiza inteligencia de amenazas de la forma convencional. (Ltd, 2015)

El documento "Inteligencia de amenazas: recopilación, análisis, evaluación" (Ltd, 2015), propone un modelo diferente en el desarrollo de inteligencia de amenazas, definiendo cuatro categorías distintas basadas en el consumo de información. Estas categorías son las siguientes:

La Inteligencia Estratégica de Amenazas, corresponde a la información de alto nivel, consumida o usada en niveles altos de dirección; es decir por todos aquellos responsables en la toma de decisiones. No debe ser técnico y debe contemplar impactos financieros ocasionados por la actividad cibernética, el usual corresponde a que las tendencias de un ataque que podrían tener un impacto en las decisiones empresariales de alto nivel, por lo que un consejo debería tener presente los beneficios y los riesgos de esta forma se asignan esfuerzos y presupuesto para mitigar los ataques esperados de este tipo.

La inteligencia de Amenaza Operacional, esta corresponde al manejo de información relacionada con ataques definidos que van en contra de la organización y es gestionada en primera instancia por las personas de seguridad de alto nivel, como los administradores de seguridad o los encargados de respuesta a incidentes. El desarrollo de capacidades y la buena gestión de este tipo de amenaza permiten resolver las respuestas planteadas en un incidente respecto a quien, como, y cuando, en los ataques, el poder desarrollar implica la identificación de diversas fuentes.

La Inteligencia de amenaza táctica, esta hace referencia a tácticas, técnicas y procedimientos (TTPs) y es información de cómo los actores de la amenaza realizan los ataques.

La inteligencia de amenaza táctica es aplicada por los entes encargadas de mantener y realizar defensa y respuesta, manejo de alertas y se encargan de realizar e investigación. Sobre este tipo de inteligencia se deberá centrar inicialmente la investigación para el desarrollo de proyecto definido. (Ltd, 2015)

La inteligencia de amenaza técnica es la información obtenida mediante medios técnicos la información aquí obtenida tiene una vida corta debido a la dinámica, por ejemplo, las direcciones IP o la modificación de las huellas digitales del tráfico de red o de archivos, esto implica la conveniencia de implementar mecanismos automáticos para su obtención. El propósito de esta inteligencia se enfoca en proveer de elementos en la realización de investigaciones o supervisiones de una empresa.

De manera general el modelo que se toma como base para el desarrollo del presente documento, consta de varias etapas que en su implementación aplica lo que se llama el "círculo de la inteligencia" (Ltd, 2015) que consta de los siguientes pasos de acuerdo con el autor que explican como parte del contexto del desarrollo del documento:

Requisitos: Este paso busca generar una guía para poder identificar de quienes toman decisiones que quieren saber respecto a las tecnologías de la información, que información

quieren recibir. En la lectura se muestran dos ejemplos que aplican para el entendimiento de la etapa indica que la dirección en donde la dirección quiere tener información sobre las vulnerabilidades públicamente conocidas y ampliamente explotadas.

Recolección: Este punto se define como aquel en donde se va la mayor parte del presupuesto en TI, aquí se busca recopilar toda la información y los datos para identificar la información esperada posterior a su análisis. Los datos pueden provenir de diferentes fuentes que incluyen tecnología e incluso intervención humana. En esta etapa es muy importante entender cuáles son las fuentes que podrían ser la información que se desea, este punto es muy importante en el desarrollo del ciclo.

Análisis: Esta etapa se encarga de transformar los datos obtenidos en información, este análisis puede llegar a ser simple en algunos casos donde se miren reglas o complejo en otros casos donde requiere extraer los datos. En este paso es posible se identifiquen oportunidades que permitan crear nuevos tipos de inteligencia, en otros casos es posible que no lleve a ninguna información relevante.

Producción / Difusión: Esta etapa realiza la creación y transmisión de resultado de la inteligencia a los clientes; es el producto.

Evaluación: En esta etapa se realiza una evaluación del producto obtenido, buscando asegurar que cumple con los requisitos solicitado desde un inicio, permitiendo desarrollar nuevos

requisitos de mayor profundidad y el ciclo de inteligencia puede repetirse. En caso de que el producto no cumpla con los requisitos solicitados, entonces indicaría un fallo en algún momento, y el modelo de ciclo puede usarse para establecer y redefinir requisitos, fuentes, datos, análisis, o el producto final.

Modelos para identificación de Amenazas

Las diferentes técnicas de defensa en la red que aprovechan el conocimiento sobre sus adversarios, pueden crear un ciclo de retroalimentación de inteligencia, permitiendo a los defensores tener un nivel superior, disminuyendo la probabilidad de éxito del adversario (Hutchins, Clopperty, & Amin).

El uso de un modelo para describir fases de intrusiones, mapear indicadores adversarios identificar posibles cursos de acción, identificar patrones y comprender la naturaleza iterativa de la recopilación de inteligencia desde la base de la defensa de redes informáticas reduce la probabilidad de éxito del atacante, permiten identificar mecanismos de defensa en la red y la priorización de recursos, y arroja métricas relevantes de rendimiento y efectividad (Hutchins et al.). Este modelo mitiga no solo la vulnerabilidad, sino también el componente de amenaza de riesgo (Hutchins et al.).

Uno de los modelos para la identificación y prevención de la actividad de intrusiones cibernéticas es llamado Kill Chain (Martin, 2015). Este modelo de defensa lo que hace es tener

en cuenta los pasos que tiene que dar un ciberdelincuente para tener éxito. De esta forma, las empresas pueden saber qué medidas de seguridad pueden establecer en cada una de las fases para garantizar una seguridad global. Y en caso de que no funcione, dónde podría haberse producido el fallo (Martin, 2015).

Kill Chain detalla en siete fases un ataque externo a una red, con ello se facilita la correlación entre cada una de las fases y las diferentes herramientas de defensa existentes (Abawajy, Mukherjea, Thampi, & Ruiz-Martínez, 2015) . Las siete fases que la forman son:

- Reconocimiento: aprender sobre el objetivo utilizando diversas técnicas (Abawajy et al., 2015).
- Creación del arma: adecuación del código malware al medio sobre el que se buscará la infección(Abawajy et al., 2015).
- Entrega: transmitir el código malware a través de algún medio (Abawajy et al., 2015).
- Explotación: aprovechar alguna vulnerabilidad en el software o error humano para ejecutar el software malicioso (Abawajy et al., 2015).
- Instalación: el software malicioso se asegura de poder ejecutarse de forma permanente en el equipo infectado (Abawajy et al., 2015).
- Comandos & Control (C2): el malware se comunica con su central, proporcionando a los atacantes control remoto (Abawajy et al., 2015).
- Acciones sobre los objetivos: se procede al robo o a la ejecución de lo que se planteara hacer (Abawajy et al., 2015).

En el desarrollo de Ciberinteligencia se requiere el uso de herramientas para la recolección y almacenamiento de grandes volúmenes de datos de los dispositivos y la correlación avanzada, basadas en reglas o anomalías de detección, después de esto es necesaria la aplicación de herramientas que permitan la identificación de estructuras de mando y control, facilitar la detección de nuevas víctimas las capacidades de los atacantes y sus procedimientos. Un proceso así, iterativo permite determinar las tácticas, técnicas y procedimientos (TTP) del atacante, al igual que su motivación (Candau, 2017).

Adaptando el ciclo de inteligencia en la ciberseguridad mediante el modelo diamante, es posible resolver cuatro aspectos básicos: (Candau, 2017)

- Identificación de la víctima: Se busca determinar la fortaleza que tenga para resistir cualquier ataque, sus capacidades de detección, las vulnerabilidades que permiten el despliegue del atacante o las medidas de seguridad implementadas (Candau, 2017).
- Capacidades técnicas del atacante: Identificar los vectores de infección, las vulnerabilidades conocidas del fabricante, capacidades de despliegue por la red, capacidades de ocultación y persistencia (Candau, 2017).
- Infraestructura utilizada: Identificación de la infraestructura, protocolos empleados para la comunicación (Candau, 2017).

- Identificación del atacante: Catalogar el tipo de agente que lo realiza (estado, crimen organizado, ciberactivistas, actores internos, empresas competidoras, etc.) (Candau, 2017).

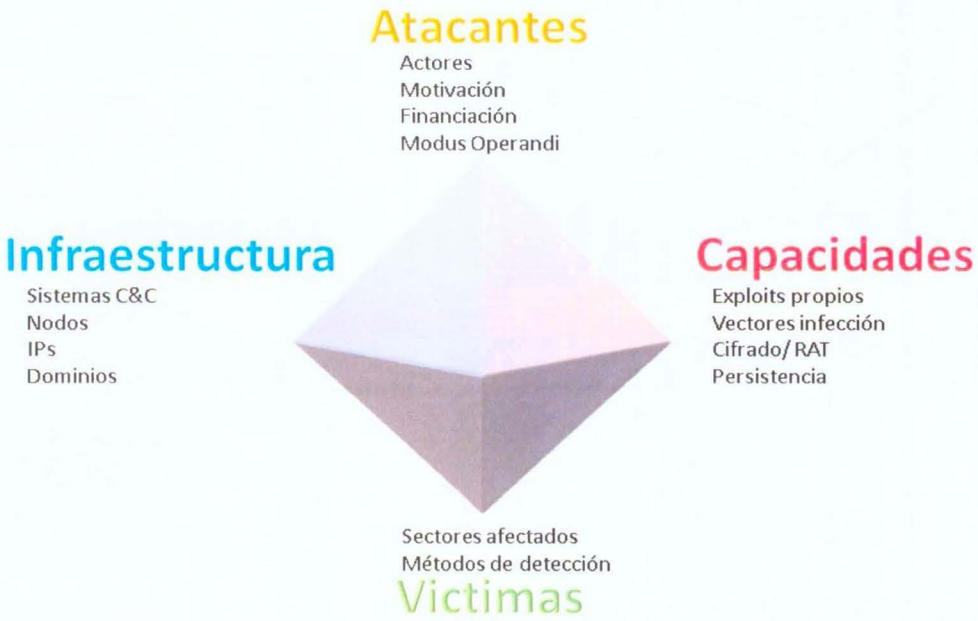

Ilustración 1 Modelo Diamante

El análisis del modelo diamante en relación vertical (socio-económica) entre víctima y atacante permite alcanzar conclusiones estratégicas (y llega a la identificación del actor); mientras que la relación horizontal (técnica), posibilita la mejora de la capacidad de detección y respuesta de la parte defensiva (Candau, 2017).

La actividades que el adversario dirige contra su víctima se compone de una cadena de eventos, en un conjunto ordenado de fases que deben ejecutarse satisfactoriamente para alcanzar el objetivo final (Nacional, 2015).

La representación de los eventos en cada fase se puede realizar mediante lo que se denomina Hilo de Actividad, el cual es un grafo que contempla las del Kill Chain, donde cada nodo es un evento y los arcos identifican relaciones causales entre tales eventos(Nacional, 2015).

Ilustración 2 Hilo de Actividad

El modelo de diamante permite identificar el proceso del adversario, el cual resulta de agrupar hilos de actividad que comparten ciertas características en común (Nacional, 2015).

Un grafo de actividad-ataque facilitan el desarrollo de estrategias de mitigación más adecuadas, toda vez que contemplan coherentemente el aseguramiento de la información y la inteligencia de amenazas, integrando lo que efectivamente ha ocurrido con lo que podría ocurrir, y posibilitando una estrategia que, contrarrestando la amenaza actual, desarrolle un plan de reacción frente a movimientos futuros del adversario. Es posible crear un Grupo de Actividad, resultado de un conjunto de Eventos e Hilos de Actividad construido con un grado de confianza (Nacional, 2015).

El soporte a la generación de hipótesis, documentación y prueba constituye una de las características más importantes de los Hilos de Actividad, el primer paso del análisis debe ser definir con precisión la pregunta o cuestión para la que se desea obtener respuesta. Una vez que la cuestión ha sido planteada, pueden generarse las hipótesis, documentarse y, finalmente, probar su viabilidad (Nacional, 2015).

El desarrollo de grafo permitirá establecer hipótesis más acertadas al trabajar con un conjunto de Eventos e Hilos de Actividad asociados por características o Procesos del Adversario similares (Nacional, 2015).

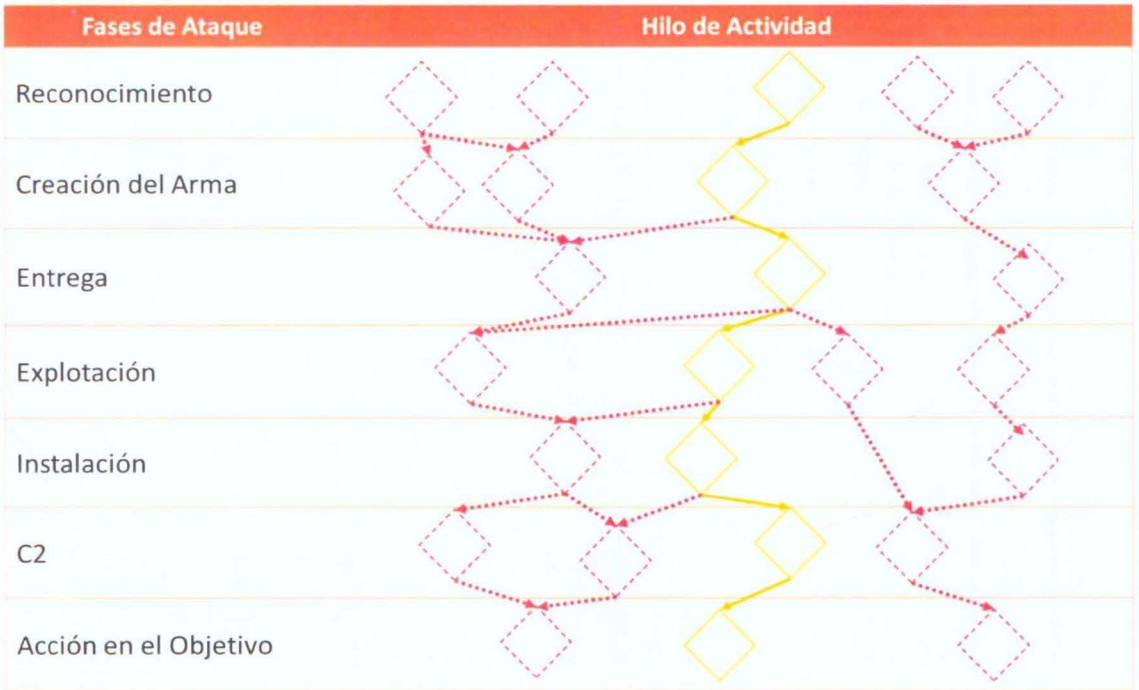

Ilustración 3 Grafo de Actividad - Ataque

En la ciberinteligencia posterior a la definición de hipótesis es posible predecir las características del ataque y los posibles indicadores, de tal forma que si se presentan es posible identificar que se está dando el ataque. Sin embargo, no todos los indicadores son iguales y algunos de ellos son mucho más valiosos que otros.

Para ilustrar este concepto, se ha creado lo que se llama la Pirámide del Dolor. Este diagrama muestra la relación entre los tipos de indicadores que son posibles de usar para detectar las actividades de un adversario y cuánto dolor le causará cuando se es capaz de negar los indicadores (Bianco, 2013).

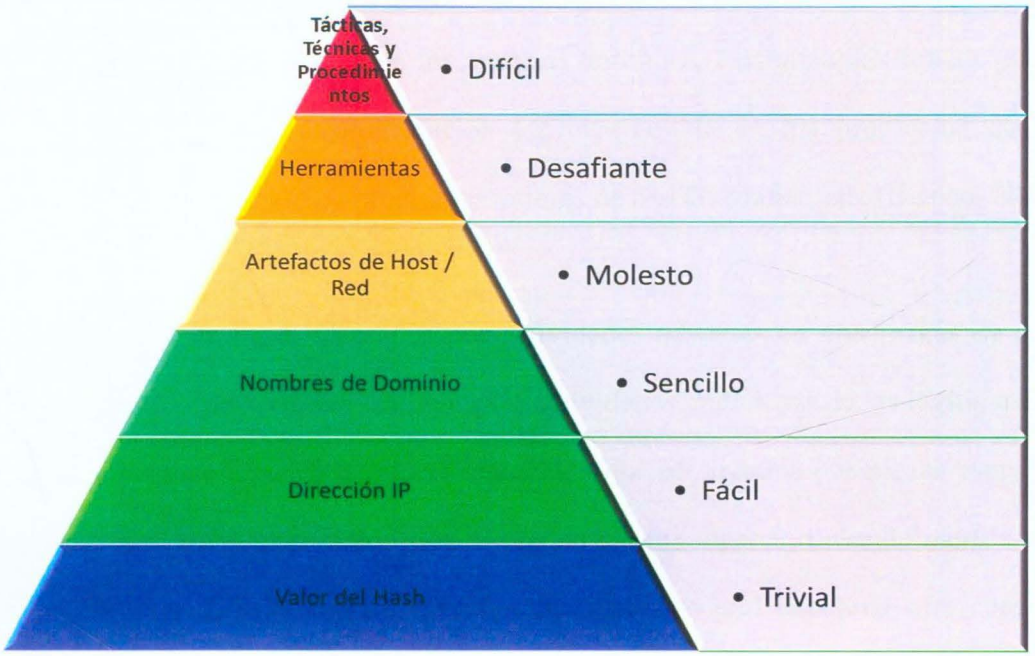

Ilustración 4 Pirámide del Dolor de David J Bianco

1. Valores hash: SHA1, MD5 u otros valores hash similares tomados de archivos sospechosos o maliciosos específicos. A menudo se utiliza para proporcionar referencias únicas a muestras específicas de malware o archivos involucrados en una intrusión (Bianco, 2013).

2. Direcciones IP: Es una dirección IP (Bianco, 2013).

3. Nombres de dominio: Puede ser un nombre de dominio o subdominio (por ejemplo, "this.is.sooooo.evil.org") (Bianco, 2013).

4. Artefactos de red: Causados por actividades adversas en su red. Técnicamente corresponde a los elementos de la actividad que podrían tender a distinguir la

actividad maliciosa de la de los usuarios legítimos. Los ejemplos típicos pueden ser los patrones URI, la información C2 incorporada en los protocolos de red, los distintivos HTTP User-Agent o los valores de SMTP Mailer, etc. (Bianco, 2013).

5. Artefactos de Host: Causados por actividades adversas en uno o más de tus hosts. Elementos que permiten distinguir las actividades maliciosas de las legítimas. Podrían ser claves de registro o valores conocidos por ser creados por piezas específicas de malware, archivos o directorios caídos en ciertos lugares o usando ciertos nombres, nombres o descripciones o servicios maliciosos o casi cualquier otra cosa que sea distintiva (Bianco, 2013).

6. Herramientas: Software utilizado por el adversario para cumplir su misión. Software o comandos que ya estén instalados en la computadora. Esto incluiría las utilidades diseñadas para crear documentos maliciosos para ataques, puertas traseras utilizadas para establecer crackers C2 o contraseñas u otras utilidades basadas en host que puedan querer utilizar después de un compromiso (Bianco, 2013).

7. Tácticas, técnicas y procedimientos (TTP): Cómo el adversario realiza su ataque, desde el reconocimiento hasta la exfiltración de datos y en cada paso intermedio. No corresponde a herramientas específicas, ya que hay varias formas de convertir un ataque (Bianco, 2013).

Indicadores de Compromiso

Existen tecnologías en desarrollo que permite en su aplicación combatir ataques cibernéticos, estas tecnologías es lo que se conocen como indicadores de compromiso (*IoC*), proporcionando herramientas donde sea posible encontrar alertas sobre amenazas descubiertas por anomalías, ataques o vulnerabilidades expuestas identificadas, creando una caracterización técnica del elemento que ocasiona dicha anomalía para luego ser compartida como una alerta. Una vez difundida esta inteligencia a las entidades, estas pueden cambiar sus tácticas defensivas buscando contrarrestar las amenazas sobre las cuales no estaba preparada inicialmente. Además, involucra para su funcionamiento los temas de intercambio de información, colaboración y gestión de incidentes descritos anteriormente, mediante la implementación de plataformas.

El desarrollo de tecnologías que implementan el uso de indicadores de compromiso apoya en el desarrollo de inteligencia de amenazas, estas tecnologías buscan mediante su uso, cumplir el propósito de mitigar de formas anticipadas la afectación de amenazas cibernéticas en las organizaciones, en diferentes aspectos los cuales son desarrollo por la academia y por empresas del sector de seguridad, las cuales serán descritas a continuación para el desarrollo del proyecto, producto de este documento:

OpenIOC fue diseñado por la empresa MANDIANT con el propósito inicial que de sus productos codificaran inteligencia buscando rápidamente brechas seguridad. MANDIANT ha dado la posibilidad de dar un esquema de uso abierto y está lanzando herramientas y utilidades

para permitir la comunicación de información de amenazas a la velocidad de la máquina. Como tal es un esquema XML en el cual se describe las características técnicas que identifican una amenaza conocida.

The Vocabulary for Event Recording and Incident Sharing (Veris), es el vocabulario para la grabación de eventos y el intercambio de incidentes, corresponde a un conjunto de métricas creadas para proporcionar un lenguaje común en la descripción de incidentes de seguridad de una manera estructurada y repetible. Permite recopilar información útil relacionada con incidentes de forma anónima y responsable con otras organizaciones. El objetivo general es crear una base para aprender constructivamente y de forma cooperativa experiencias para poder medir y gestionar el riesgo.

Cyber Observable Expression CybOX™, proporciona una estructura que permite representar eventos observados entre las áreas operacionales de la seguridad cibernética de las empresas, es un lenguaje estructurado que permite la especificación, captura, caracterización y comunicación de eventos o propiedades observables en el ámbito operacional.

El Formato de Intercambio de Objeto de Incidente (IODEF), define la forma de representar datos proporcionando un marco que permita compartir información por equipos de respuesta respecto a incidentes de seguridad informática

Trusted Automated Exchange Of Indicator Information (TAXII), define un conjunto de servicios que permiten el intercambio de mensajes compartiendo información de amenazas cibernéticas, define conceptos, protocolos e intercambios de mensajes para la detección, prevención y mitigación de amenazas cibernéticas, permite mejorar la conciencia situacional sobre las amenazas emergentes y permite a las organizaciones compartir fácilmente la información que eligen con los socios que eligen. Los casos de uso de TAXII incluyen:

Alertas o advertencias públicas

Alertas e informes privados

Empuje y retire la difusión del contenido

Establecimiento y gestión del intercambio de datos entre las partes

STIX (Structured Threat Information eXpression), es un lenguaje de programación XML creado para transmitir datos sobre amenazas de seguridad cibernética en un lenguaje común que puede ser fácilmente comprendido tanto por los seres humanos como por elementos de tecnologías enfocadas a la seguridad. Su diseño tiene un uso amplio, sin embargo, se enfoca en el análisis de amenazas cibernéticas y la actividad relacionada al respecto. También, es usado para identificar patrones que podrían materializar una amenaza cibernética.

Traffic Light Protocol (TLP), define un esquema sencillo e intuitivo que permite indicar cuándo y cómo se puede compartir información confidencial, de esta forma busca facilitar una colaboración más frecuente y eficaz. No es un "marcado de control" sobre la información ni corresponde a un esquema de clasificación. Su propósito principal es facilitar un mayor

intercambio de información. Emplea cuatro colores para indicar los límites de reparto esperados que deben aplicar los destinatarios.

Open Threat Exchange, Es una comunidad de inteligencia de amenazas abierta que busca crear defensa colaborativa con datos de amenazas reportadas por una comunidad. El propósito es que las compañías y agencias gubernamentales recopilen y compartan información relevante, oportuna y precisa sobre ataques cibernéticos nuevos o en curso lo antes posible para evitar brechas importantes (o minimizar el daño de un ataque).

Collective Intelligence Framework, es un sistema de gestión de inteligencia de amenazas cibernéticas que permite combinar la información de amenazas maliciosas conocida de muchas fuentes y utilizar esa información para identificación (respuesta a incidentes), detección (IDS) y mitigación (ruta nula). Los tipos más comunes de inteligencia de amenazas almacenados en CIF son direcciones IP, dominios y URLs que se observan están relacionados con la actividad maliciosa.

Normatividad

Existen una preocupación por el riesgo que existe en el uso de las redes informáticas utilizadas para cometer delitos y en el almacenamiento y trasmisión de pruebas por dichas redes, a la vez se reconoce que la lucha con la ciberdelincuencia requiere de una gran cooperación.(Europe, 2001)

Hoy en día el desarrollo de convenios es necesario para prevenir los actos que pongan en peligro la confidencialidad, integridad y disponibilidad de datos, redes y sistemas informáticos. (Europe, 2001)

El desarrollo normativo y jurídico debe tomar como referencia un convenio que tenga un reconocimiento como el de Budapest. Este convenio tiene presente incorpora todos los convenios existentes del consejo de Europa de cooperación en materia penal, y otros tratados con el fin de incrementar la eficacia de las investigaciones y procedimientos penales relativos a los delitos relacionados con sistemas y datos informáticos, así como prevenir la obtención de pruebas electrónicas de los delitos. (Europe, 2001)

Para las entidades miembro del Comité de coordinación para el seguimiento al sistema financiero es crucial el cumplimiento de sus objetivos, para esto deben realizar mejoras técnicas de los medios y procedimientos utilizados en relación con el seguimiento del sistema financiero (E. M. d. H. y. C. Público, 2003) , esto indica mantener aislado de su operación lo que podría ser un ataque cibernético.

Para las entidades miembro del comité, es conveniente crear un grupos de trabajo interinstitucional, que permitan desarrollar estudios o análisis de temas de interés que contribuyan al cumplimiento de sus objetivos (M. d. H. y. C. Público, 2014), uno de estos grupos debe enfocarse mitigar afectaciones por ataques cibernéticos ya que podría afectar el cumplimiento de sus objetivos.

Es posible la definición de convenios especiales de cooperación con el fin de fomentar el desarrollo de actividades tecnológicas y la creación de tecnologías, además de poder aportar recursos de distinto tipo para facilitar, fomentar, desarrollar y alcanzar en común algunos propósitos.(Planeación, 1991)

CAPITULO 2. CREACIÓN DE GRUPOS PARA RED DE COLABORACIÓN

Para el desarrollo de mecanismos de colaboración, el enfoque inicial se debe orientar en la búsqueda de ganancia para las partes que intervienen, esta ganancia no necesariamente debe ser económica, de esta forma se genera un mayor interés y compromiso.

Desarrollar el proceso de colaboración sin la identificar la ganancia, llevaría a desmantelar alguna estructura planteada por la inexistencia de un interés real, generado incluso perdidas a todas las partes involucradas por su inversión en tiempo, personas o económicos que conclusión afectan el resultado definido en principio.

Generar una red de colaboración basada en el desarrollo de una etapa filantrópica es difícil, la obtención de recursos se basa en la búsqueda de donaciones de recursos, afectando tiempos relacionados con resultados del proyecto (definición de filantropía en la RAE). La filantropía no es usual para el desarrollo de proyectos tecnológicos y/o de seguridad. La aplicación de una etapa filantrópica puede ser contemplada en algún momento para una posible mejora de un proyecto en funcionamiento, entregando como retribución una promoción de imagen del benefactor y apoyándolos o resaltando el desarrollo de sus valores como responsable y comprometido (Romero et al., 2005).

El desarrollo de una etapa transaccional, en la cual existe interacción por la realización de las actividades específicas, busca que el resultado sea el producto de un importante intercambio bilateral de valor, de esta forma se obtienen beneficios para las partes sin que necesariamente sean los mismos. Esto fomenta y permite un intercambio de capacidades generando una relación que pasa a ser importante para los involucrados. El desarrollo de esta etapa genera mayor interacción debido a los intereses y la búsqueda del resultado, permite desarrollar gestión ordenada y especifica por la inversión de recursos. (Romero et al., 2005)

Es de mayor conveniencia para el proyecto, desarrollar una etapa transaccional debido a que el enfoque inicial se orienta en un desarrollo colaborativo, buscando se genere la ganancia para todos los que hacen forman parte. Es posible obtener mayor interés cuando se desarrolla desde el punto en el que se alimente la estrategia de cada participante, creando alianzas estratégicas con misiones conjuntas, sincronizados estrategias y creando valores compatibles. De esta forma los integrantes realizan interacción con mayor frecuencia y desarrollan una mayor cantidad y variedad de actividades en común.

De esta forma se podrían ver las capacidades de cada entidad de forma multiplicada, con mayores recursos, en este caso la competencia entre las partes no aplica tan solo convergen creando valor debido a la integración organizacional. En este tipo de casos es usual que el desarrollo de estrategias conjuntas portando de forma constante y colaborativa.

El principal motivador para participar en la definición de estrategias colaborativas se encuentra la mitigación de riesgos con el fin de mitigar la posibilidad de ocurrencia de diferentes hechos o

evitar consecuencias negativas, la participación con este propósito es usual en entidades que ocupan una posición de liderazgo y con alto grado de afectación por temas de imagen reputacional.

El desarrollo de una red de colaboración multiplicando capacidades, permite competir contra la contraparte que no podemos perder de vista ya que corresponden a los delincuentes o criminales del ambiente cibernético.

El desarrollo de una estrategia en una etapa integrativa, busca el desarrollo de una sola estrategia, misión y en los valores conjuntos, el incentivo es mayor debido a que corresponde a minimizar impactos por riesgos del ciberespacio afectando un sector o un país, sin afectar la identidad de cada participante. Cuando el resultado de la colaboración es muy relevante para el sector o el país, esta sinergia adquiere importancia estratégica sectorial, lo que en cierta forma crea la necesidad de crear y mantener fuertes incentivos para mantener el compromiso y asignar más recursos permanentes.

La información que se transmite es la base de la colaboración, debido a que esta origina el verdadero valor de mantener la cooperación, por esto la comunicación debe ser constante y efectiva, debe ser realizada lo más prontamente posible creando así las advertencias sobre la amenaza para la realización de acciones preventivas. Mantener el anonimato sobre las comunicaciones que se generen permitirá no solo no identificar la entidad afectada sin perjudicar su reputación, sino, que además evita la generación de prejuicios sobre la participación.

Debe existir no solo un compromiso de participar como receptor de alertas, sino que además debe existir un compromiso de reportarlas, por esta razón se definen dos elementos importantes para la participación en la red de colaboración, el primero corresponde a que la entidad debe generar estrategia siendo parte de la red de colaboración, mostrando la ganancia de participar en la red y además debe mantener un mecanismo de gestión de incidente donde se pueda identificar los eventos o incidentes de origen cibernético. De esta forma será posible identificar la participación mediante la comparación de los eventos registrados y los eventos reportados en la red de colaboración.

Es importante tener presente que el propósito es crear una base que permita en algún momento expandir la red de colaboración, es decir; que se amplié el número de partes llegando a obtener más alertas creando mayor efectividad. La efectividad en los reportes que se realicen permitirá minimizar efectos negativos por ataques cibernéticos y mantendrán el compromiso de formar parte de la red de colaboración.

La implementación de una red de colaboración que se alimenta de la información de origen de fuentes humana es considerada como una estrategia base, si el alcance se extiende generando aprovechamiento global, debido a que los ciberdelincuentes se encuentran en cualquier parte del mundo, creará mayores dificultades para los atacantes. El aprendizaje sobre todos los eventos e incidentes debe ser otro motivante que llame la atención y que convoque a más participantes, llevando a la mejorar continua en los procesos y a controles más efectivos.

El desarrollo de una red de colaboración donde cada parte tenga clara su responsabilidad y sus compromisos sobre los cuales se basan sus tareas, no requerirá de líderes que indiquen el camino, se orienta a la realización de sus tareas lo que es una gran paso al desarrollo de una inteligencia colectiva, de esta forma seria posible tener mayor utilidad para cada miembro optimizando procesos.(Torres, 2014)

Este proyecto busca generar un enfoque incluyente y de colaboración involucrando no a un sector específico, sino a múltiples partes interesadas promoviendo la seguridad digital y aumentando las capacidades frente a eventos o incidentes (**CONPES 3854**). De esta forma se promueve la colaboración y la cooperación, y se incrementa las capacidades y el fortalecimiento frente a la gestión del riesgo de la seguridad digital (**CONPES 3854**).

Es usual que existan mayor número de elementos en común cuando se habla de un mismo sector, existiendo la posibilidad que las causas y vulnerabilidades en sus elementos se presenten en otra entidad. La aplicación de este proyecto se orienta inicialmente al Grupo de Coordinación de Seguridad del Sistema Financiero del cual hace parte el Ministerio de Hacienda, el Banco de la República, la Superintendencia Financiera y el Fondo de Garantías de Instituciones Financieras; sin embargo, es posible se aplique a cualquier otro sector o subsector existentes dentro de los diferentes sectores económicos del país aplicando lo definido por el Conpes 3854, estos sectores pueden ser (República, 2015):

1. Sector agropecuario
2. Sector de servicios
3. Sector industrial
4. Sector de transporte
5. Sector de comercio
6. Sector financiero
7. Sector de la construcción
8. Sector minero y energético
9. Sector solidario
10. Sector de comunicaciones

Caracterización de Elementos en Común:

Los eventos o incidentes que los miembros de la red de colaboración deben reportan, son todos aquellos que se identifican que buscan crear una afectación sobre los activos de información[1], lo que indica la importancia de estos.

La entidad participante debe primero identificar los activos que pueden ser afectados, para apoyarse es conveniente la realización de un inventario que debe mantener actualizado, además, puede ser usado con otros propósitos, ejemplo gestión del riesgo.

---

[1] Un activo de información en el contexto de un SGSI y con base en la norma ISO/IEC 27001:2005 es: "algo a lo que una organización directamente le asigna un valor y por lo tanto la organización debe proteger"(ICONTEC, 2006)

En primera instancia se debe realizar un inventario de los activos que pueden ser afectados por ataques cibernéticos, este inventario debe ser gestionado por la entidad y se debe diligenciar en un formato como el siguiente.

Tipo de Elemento	Nombre del Elemento	Fabricante	Referencia	Versión/Serie	Propósito

Tabla 1 Formato de Identificación de Activos.

En este formato se encuentran los siguientes campos:

- Tipo de elemento, este identifica si el activo a registrar corresponde a software, servidores, almacenamiento, redes o seguridad.
- Nombre del elemento, este campo identifica el nombre que tiene, como tal es el elemento, ejemplo servidor, switch, página web, procesador de texto, etc.
- Fabricante, este campo identifica el nombre del fabricante del activo, no se debe confundir con el distribuidor.
- Referencia, en este campo corresponde a la referencia del activo
- Versión / Serie: indica la referencia y/o serie del tipo de activo.

- Propósito, corresponde a la función que desempeña el activo, para este caso debe indicar si es base de datos, sistema operativo, telecomunicaciones, página web, aplicación.

Las siguientes tablas corresponde a tipo de elementos (Focus, 2017), que deben ser referenciados en los inventarios que se realicen, en caso de tener un activo que obedece a las tablas siguientes, podrá ser ingresado en el inventario de acuerdo a como sea interpretado por quien realice el registro de los elementos (Inc., 2014):

Tipo: Software

Gestión del ciclo de vida de las aplicaciones
Gestión de la entrega de aplicaciones
Análisis de grandes datos
DevOps
Seguridad Empresarial
Nube híbrida y privada
Gobierno de la Información
Gestión de la información
Gestión de servicios de TI
Jefe de operaciones
Administración del servidor
Software como servicio (SaaS)
Centro de datos definido por software
Administración de almacenamiento

Tabla 2 Tipo Software

Tipo: Servidores

Servidores de bastidor
Servidores de torre
Servidores Blade
Densidad optimizada
Servidores de misión crítica
Servidores para Cloud
Administración del servidor

Tabla 3 Tipo Servidores

Tipo: Almacenamiento

Almacenamiento todo-flash e híbrido
Almacenamiento medio y empresarial
Sistemas de almacenamiento de entrada
Disponibilidad de datos, protección y retención
Almacenamiento Definido por Software
Gestión y orquestación
Redes de almacenamiento

Tabla 4 Tipo Almacenamiento

Tipo: Redes

Interruptores
Routers
Puntos de acceso y controladores
LAN inalámbrico
Redes de campus y sucursales
Redes de centros de datos
Red de área amplia
Redes definidas por software
Funciones de red Virtualización
Administración de redes

Tabla 5 Tipo Redes

Tipo: Seguridad

Firewall
IDS
IPS
Control de Acceso a Redes (NAC)
UTM
Antimalware
Protección de Email
Firewall de Aplicación Web (WAF)
Sistemas contra APT
Sistema de intercambios de Amenazas

Tabla 6 Tipo Seguridad

La red para el desarrollo de este trabajo está conformada por el Banco de la Republica, el Ministerio de Hacienda, la Superintendencia Financiera y Fogafín, sin embargo; podrá ampliarse en una segunda fase del proyecto a otras entidades o ser incorporada en otros sectores.

La definición del grupo de trabajo debe establecer los requisitos para orientar los resultados requeridos, de acuerdo con las alianzas estratégicas definidas, además del listado de los activos y sus características se pueden definir no solo los riesgos (de acuerdo con las amenazas), sino el modelamiento de las actividades de ataque para la definición de hipótesis.

CAPITULO 3. APLICACIÓN DE LA INTELIGENCIA DE AMENAZAS

La inteligencia se basa principalmente en obtener o recolectar información en un contexto interno o externo para luego evaluarla, realizar un análisis y generar un resultado interpretado sobre elementos desconocidos, con el propósito de poder anticipar posibles eventos no deseados, para así definir posibles actividades o estrategias que busquen proteger intereses. No es una novedad la aplicación de inteligencia con el fin de contrarrestar amenazas, ya que su aplicación se considera una buena práctica. Desarrollar esta actividad requiere de un conocimiento y una preparación especializada con intervención humana por lo general dentro del proceso general (Legislativo, 2009).

El tipo de inteligencia para aplicar en el proyecto busca el desarrollo de actividades preventivas frente a amenazas que afecten la ciberseguridad de una entidad, de las cuales se identificaron que ocasionaron o pudieron ocasionar afectaciones en la información o en la infraestructura tecnológica, esto con el fin de alertar a otras entidades que tengan componentes comunes. El escenario en el que se desarrolla el proyecto es en ciberseguridad.

Para el desarrollo se consideran realizar cuatro tipos de inteligencia:

- Inteligencia Estratégica
- Inteligencia Operativa
- Inteligencia Táctica

- Inteligencia Técnica

Inteligencia Estratégica: Manteniendo la definición corresponde a la inteligencia que obtiene información para ser entregada a quienes toman decisiones, esta información no es de carácter técnico y se orienta en posibles impactos por la materialización de riesgos que pudiesen afectar decisiones del negocio de alto nivel. (Ltd, 2015). Para este caso, se deberán generar informes anuales relacionados con los riesgos que generen afectación al negocio desde el punto estratégico, estos deben ser presentados en el marco de la revisión o definición del plan estratégico.

Inteligencia Operativa: Esta inteligencia se enfoca a un nivel alto respecto a quienes gestionan los temas de seguridad, quienes responden ante los incidentes que se puedan generar, la información recibida en este nivel es de uso inminente en corto tiempo, las actividades se enfocan en contrarrestar los ataques. (Ltd, 2015). Esta información debe ser presentada a la dirección de la entidad justificando los elementos que mantienen para la seguridad de la entidad.

La inteligencia Táctica: En este nivel, la inteligencia se enfoca en la información al nivel de tácticas, técnicas y procedimientos, para identificar mediante el análisis la forma en que los atacantes realizan sus ataques, de esta forma se busca mantener preparada las defensas, alarmas y la investigación. (Ltd, 2015). Con esta información la entidad debe tener la posibilidad de evaluar el estado de sus procesos y procedimientos que permiten contrarrestar los ataque que se realizan en cada entidad.

La inteligencia Técnica: Se obtiene información técnica, esta es de uso inmediato ya que cambia rápidamente, esta debe ser consumida para su análisis de forma automática. De aquí se genera toda la información respecto a los activos objetivo y los atributos del evento, esta información debe ser reportada y usada a las entidades con funciones CERT (Computer Emergency Response Team) del estado quienes deberán investigar y generar acciones que mitiguen otros impactos. Además, permite a la misma entidad identificar elementos a incorporar en listas negras de dispositivos de seguridad evitando acciones por parte de estos.

Ilustración 5 Subtipos de inteligencia de amenazas (Ltd, 2015)

Para el desarrollo de la inteligencia, se debe desarrollar los siguientes pasos, que obedecen a un ciclo:

- Requerimientos
- Recolección
- Análisis
- Producción
- Evaluación

Ilustración 6 Ciclo de Inteligencia

Requerimientos: La dirección o mesa directiva deben identificar y tener claro que información de tecnología relacionada con las afectaciones en seguridad desea conocer, de esta forma es posible identificar sus atributos y las capacidades para su obtención.

Recolección: El origen de la información puede tener diferentes fuentes; sin embargo, para el propósito del proyecto, este debe corresponde a la identificación de eventos o incidentes que afecten a la entidad, donde se detalle la afectación.

Análisis: La información reportada debe ser analizada con el propósito de identificar los activos y sus componentes afectados.

Producción: En este paso, ya se tiene un producto de la inteligencia con el propósito de tomar acciones, para el caso del proyecto corresponde a las alarmas.

Evaluación: Aquí se realiza una evaluación del producto, de esta forma es posible identificar el cumplimiento de los requerimientos establecidos.

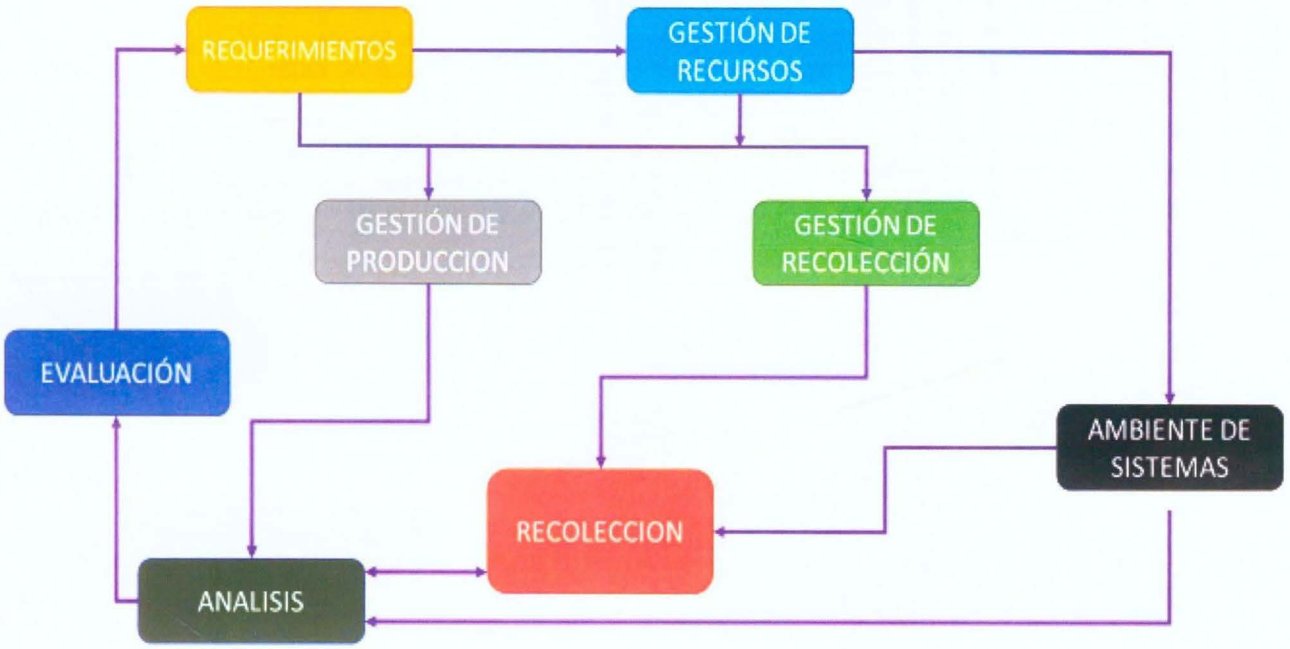

Ilustración 7 Flujo funcional de la inteligencia de amenazas

En el diagrama anterior, se identifica el flujo de las actividades involucradas de forma detallada, que permiten la interconexión de cada uno de los pasos del ciclo de inteligencia definido (Ltd, 2015), y aplicado en el proyecto.

Inteligencia Estratégica de Amenazas

En el desarrollo de la inteligencia estratégica de amenazas, el enfoque que se maneja se orienta en la información que debe llegar a la mesa directiva apoyando a la estrategia de la entidad al identificar los riesgos cibernéticos y afectaciones en aspectos técnicos.

La mesa directiva debe definir sus requerimientos de información producto de la inteligencia de amenazas, permitiéndoles tomar decisiones. Para esto, la mesa directiva debe identificar los posibles riesgos de negocio que afecten a la estrategia de la entidad, cuya causa de materialización se origina técnicamente de acuerdo con los servicios y activos, que tiene que pueden verse afectados.

El enfoque de los requerimientos de la información requerida mediante inteligencia, debe permitir que la mesa directiva tome decisiones que apoyen el desarrollo de los objetivos estratégicos y no su afectación.

En entidades del sector público, las afectaciones por amenazas cibernéticas, no deben de llevar al incumplimiento de las funciones asignadas a la entidad por la ley o a que generare afectaciones por incumplimiento normativo, legal o reputacional.

La recolección de la información en este nivel debe tener relación desde un punto de afectación del sector o del país de acuerdo con los eventos o incidentes reportados sobre los cuales se deben tomar acciones.

Para la recolección, se debe contemplar la relación de la entidad con otras entidades del mismo sector, entendiendo las afectaciones en el sector, de la misma forma que tener la afectación que podría tener la entidad por afectaciones de otras entidades.

Para este punto se realizarán reportes de forma periódica sobre los eventos o incidentes sucedidos que pueden llegar a generar una afectación técnica a la entidad. Este reporte debe permitir un análisis de afectación mediante la identificación previa de los riesgos del negocio concluyendo si existe o no alguna afectación a la estrategia.

Lo que debe seguir corresponde a la definición de un resultado o producto correspondiente a la definición de cambios en la estrategia, posibles asignaciones presupuestales, solicitudes de planes de acción de mitigación de los riegos. Varias conclusiones deben ser muy posiblemente tomadas con carácter confidencial.

Además, la mesa directiva debe retroalimentar a todas las partes con el producto o resultado, si la información analizada cumple con los requerimientos establecidos que para este caso corresponden a la identificación en la afectación de sus funciones establecidas, a su reputación o a incumplimientos normativos o legales.

Dentro de la retroalimentación debe existir información que no solo retroalimente al sistema, sino que además permita a otras entidades identificar la ganancia de la existencia de este.

Inteligencia Operativa de Amenazas

Para el nivel operativo los requerimientos sobre la información requerida, se debe centrar en los mecanismos o manera en que llegan afectarse los activos. Esta información es difícil de obtener debido a que para este proyecto la posibilidad de remitir el alcance en la identificación de las vulnerabilidades es opcional ya que si es relevante los importante para el proyecto es identifica la amenaza. Es de valor, realizar en este punto la identificación de las vulnerabilidades que existen en su infraestructura, la cuales están tratadas, en proceso o sin tratar, de esta forma el requerimiento debe permitir identificar que eventos o incidentes detectados puede llegar a afectar alguna de estas vulnerabilidades o en caso de no, el requerimiento debe llegar a solicitar la identificación de la vulnerabilidad no identificada aún.

La recolección de la información para este tipo de amenaza se debe basar en los ejercicios que se realicen para la identificación de vulnerabilidades que existen o pueden existir para cada elemento de su plataforma tecnológica, esto puede ser generado mediante pruebas internas de identificación de vulnerabilidades y mediante suscripciones a grupos de interés de seguridad. Es muy importante que se identifique al mismo tiempo el conjunto de actividades a realizar para eliminar la vulnerabilidad (planes de acción)

El análisis debe identificar de acuerdo con los reportes de alarma si alguna vulnerabilidad en tratamiento o sin tratar puede verse afectada con el fin de acelerar los planes de remediación.

El producto obtenido debe relacionarse con el tipo de vulnerabilidades que deben ser atendidas y tipo de vulnerabilidades de las cuales son susceptible en la entidad, de esta forma se genera priorización al tratamiento de un tipo específico de vulnerabilidades.

El resultado de la evaluación debe permitir compartir información a otras entidades respecto a las actividades y mecanismos usados para el tratamiento de las vulnerabilidades permitiendo identificar para el sistema que alarmas deben tener mayor relevancia.

Inteligencia Táctica de Amenazas

El desarrollo de requerimientos en este tipo de inteligencia se debe enfocar en la identificación de los mecanismos y elementos involucrados para realizar un ataque. El reporte de un evento o incidente se realiza cada vez que se genera alguna afectación sobre algún activo, este activo debe pertenecer a algún tipo de elemento a identificar y la forma en que llego la afectación debe ser reportada en términos fáciles de entender por el sistema dando información relacionada con la técnica de afectación.

La obtención de esta información se realizará mediante el reporte del evento o incidente en un campo de posibles alternativas.

Para poder analizarlo se debe identificar de acuerdo con el tipo de elemento su relación con los posibles vectores de ataque para que se analicen las alternativas.

El producto debe permitir los posibles elementos que pueden versen afectados de acuerdo con el propósito registrado en la tabla, con el fin de generar alertas de prevención y no de acción de acuerdo con el evento o incidente reportado.

Como resultado de lo anterior es conveniente identificar si es posible tener alguna materialización de estos eventos en otros tipos de elementos con propósitos similares con los tipos de activos que fueron afectados inicialmente

Inteligencia Técnica de Amenazas

El desarrollo de requerimientos busca llegar a tener toda la información técnica posible permitiendo tomar acción de forma inmediata como el ingreso a listas negras, la marcación de sitios o acciones no permitidas. En este punto se debe obtener direcciones IP públicas, nombre de archivos, asuntos de correos, hash que identifiquen la firma de los archivos, direcciones de sitios web (URL, Uniform Resource Locator) y en mayor detalle indicadores de compromiso que pueden estar compuesto por todo lo anterior.

La recolección de esta información se realiza con la aplicación del sistema que permite el registro de los indicadores de compromiso, posteriormente el sistema genera un análisis con el

registro realizado y el producto corresponde a la generación de la alarma a todas las entidades de la red de colaboración quienes posteriormente deben identificar su afectación de acuerdo con su proceso de gestión de incidentes e inventario de activos.

Como evaluación se espera obtener la información de la aplicación al igual que posibles otros hallazgos e incluso falsos positivos reportados por el sistema, de tal forma que se puede retroalimentar a todos los miembros.

Tabla 7 Aplicación de Inteligencia de Amenazas

La entrada a esta etapa es dada por las herramientas que permitan no solo reportar los eventos o incidentes, sino que además las que permiten analizar los de tal forma que responda a todos los requerimientos de los diferentes tipos de inteligencia.

CAPITULO 4. TECNOLOGÍAS Y PROCEDIMIENTOS PARA INDICADORES DE COMPROMISO

Es necesario realizar la implementación de mecanismos apoyados en herramientas que permitan la identificación de características específicas del elemento que ocasiono el ataque, esta identificación debe obedecer a la descripción de diferentes componentes del ataque, lo que indica que hasta que no exista la certeza de la existencia del elemento que genera un incidente, este no debe ser reportado.

Previo a la definición de las herramientas y sus características funcionales, se debe realizar un modelamiento de las amenazas posibles, para esto en primera instancia se cuenta con el listado de los elementos en común y la definición de posibles estrategias conjuntas.

El Modelamiento se realiza mediante la aplicación del Modelo Diamante, con la aplicación es posibles la definición de hipótesis identificando afectaciones de acuerdo con el desarrollo de grafos de actividad de ataque y a la identificación de atacantes, victimas infraestructura y capacidades.

Este modelo debe estar retroalimentado con los eventos e incidentes que ocurren a medida que se presenten, de tal forma que esto permitirá validar, complementar y crear hipótesis.

La definición de hipótesis debe llevar a la caracterización de elementos que ocasionan los ataques y los patrones de identificación de estos mismos, para la realización de esto es conveniente aplicar un modelamiento de estas características, de esta forma es posible definir y acordar entre los participantes de la red los indicadores a compartir.

El evento o incidente que afecto o pudo afectar a la organización debe ser analizado en marco de la gestión de un proceso de interno de incidentes, lo anterior indica que uno de los productos del proceso de gestión de incidentes debe ser la caracterización del elemento fuente del posible ataque.

El evento es la unidad de intercambio, es decir que corresponde a la información que se tiene para compartir a las miembros de la red de colaboración. Esto hace que el tipo de solución sea distribuida y depende de los miembros de la red sobre quienes debe existir una relación de confianza previa establecida para dar el carácter de seriedad y validez sobre la información que se reporte.

El modelamiento de las características define los indicadores de compromiso, además informa al proceso de gestión de incidentes los patrones de ataques que se pueden presentar para incorporarlos en el proceso de gestión de incidentes buscando el detalle para el reporte y para la automatización en la detección, para este modelamiento se aplica la Pirámide del Dolor

Para el desarrollo de la identificación de las características de evento o elemento; se usan los indicadores de compromiso (IoC), que indican los patrones que deben existir para que se presente el mismo evento o ataque, de tal forma que al momento de presentarse estos patrones lo siguiente corresponde a la generación de la alerta para el desarrollo de medidas de contención y bloqueo.

Las entidades que hacen parte de la red deben implementar herramientas de apoyo en la gestión de indicadores de compromiso. Las características de las herramientas a implementar debe ser el resultado de la identificación de la compatibilidad, capacidad y operatividad en la entidad.

Las herramientas deben permitir:

- La creación de Indicadores de Compromiso.
- Identificar la existencia de los patrones (IoC) en una plataforma.
- Almacenamiento de los Indicadores de Compromiso reportados y validados.

Al identificar los patrones de elemento usualmente se identifica:

- Nombre de archivo.
- Nombre del servicio.
- Tamaño del archivo.
- Rutas de directorio.
- Claves de registro.
- Nombre de dominio.

- Direcciones IP.
- Puertos, etc.

Un ejemplo para la creación de IoC en línea se puede ver en la Ilustración No 8 (Bluecloud, 2014), mediante este editor en línea, es posible crear expresiones que se basan en atributos de eventos. La creación de un indicador de compromiso se realiza mediante la identificación de la presencia de patrones o atributos del evento, no se requiere la existencia de todos los patrones, además, su combinación se realiza mediante el uso de operadores booleanos.

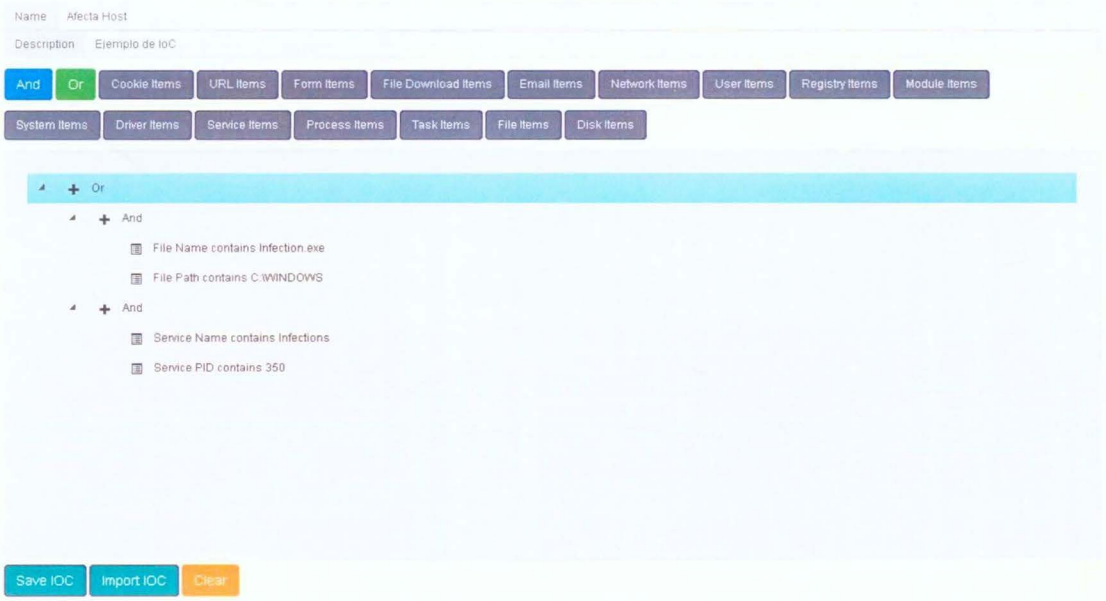

Ilustración 8 Ejemplo generador de IoC

Es conveniente en el reporte, calificar el evento de acuerdo con el impacto que ocasiono o pudo generar al momento de identificar el evento.

Para la mayoría de herramientas de gestión de Indicadores de compromiso de código abierto, los formatos estándar de mayor uso corresponden a .ioc o .yara, por tal razón la herramienta a implementar de acuerdo al marco teórico debe permitir trabajar con estos tipos de formatos para el reporte de evento y el cargue o importación de los indicadores de compromiso.

La herramienta que se implemente en la entidad miembro debe tener una conexión mediante un canal tipo VPN cifrado con la central de procesamiento para el intercambio de la información, además debe desarrollar un manual procedimental para la implementación de la tecnológica requerida para la custodia de la información en Bases de Datos, para la conexión segura entre los componentes, para el reporte entre entidades y el reporte entre bases centrales.

Es importante la identificación de componentes y elementos principales en una entidad que pueden afectar la seguridad de esta para lo cual debe mantener e implementar un procedimiento o guía que permita la realización de este paso.

La implementación de herramientas ya desarrolladas para el intercambio de información debe permitir mantener una comunicación constante y estables que permite el reporte y replica de información de eventos e incidentes de forma automática y manual para entidades con mismas características en sus componentes.

La herramienta por implementar debe definir los componentes técnicos y procedimentales que permitan descomponer cada evento o incidente del ataque, obteniendo

características detalladas de todos los elementos actores, que intervinieron y fueron comprometidos para reportarlos a una base de datos secundaria que reporte a una central, para una posterior alerta a los componentes que conforman la red, conservando el anonimato del afectado, manteniendo la veracidad del evento

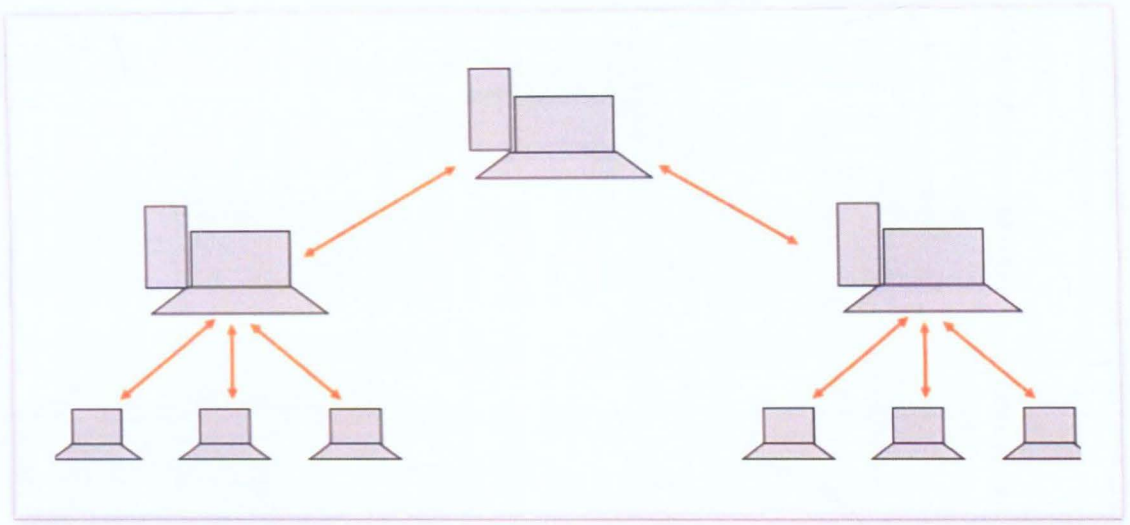

Ilustración 9 Esquema deseado

Un esquema en el cual se busca tener un servidor central o una central de procesamiento se muestra en la Ilustración No 9, aquí los eventos son centralizados y validados en un nodo central de la red, sin embargo; las diferentes tecnologías indican que una topología de red tipo araña donde todos tienen conexión con todos los servidores de la red es más efectivo y menos operativo.

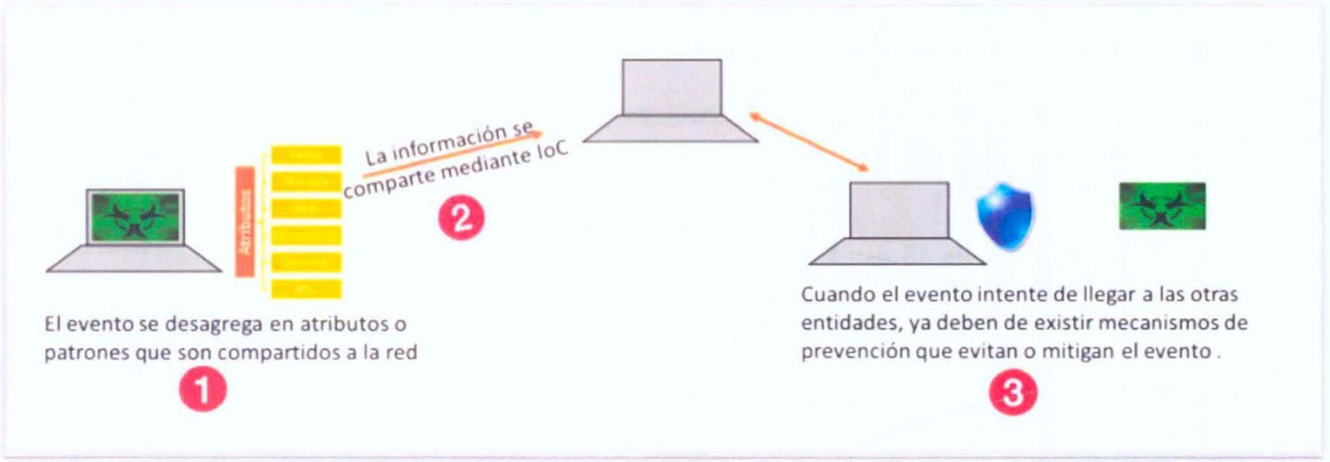

Ilustración 10 Esquema Propósito de AmeComp

Sin importar la topología de conexión a la red, lo importante es que se mantenga el propósito de implementar una de inteligencia de amenazas, tal como se muestra en la ilustración No 10.

La ocurrencia de un evento o incidente debe retroalimentar no solo el modelamiento de las amenazas aplicado mediante el modelo diamante, también debe activar el registro y reporte en la herramienta que se defina para el intercambio de la información basada en IoC.

CAPITULO 5. LINEAMIENTOS PARA LA GESTIÓN DE AMENAZAS CIBERNÉTICAS E INCIDENTES.

El desarrollo informático de cualquier entidad implica el uso de elementos tecnológicos ampliando las posibilidades de presentar diversas amenazas en la gestión de estos elementos. Es conveniente al respecto poder realizar la implementación de una estrategia de defensa que sea proactiva involucrado que como parte de esa estrategia aspectos de inteligencia que es lo que se busca de esta forma es posible para las entidades no afectadas identificar la amenaza de forma previa y eficientemente.

Para las entidades que participaran en el proyecto dentro del alcance definido, es posible el desarrollo de convenios especiales de cooperación facultados por la normatividad vigente (Decreto 393 de 1991). Este convenio en debe estar enfocado en el desarrollo de actividades tecnológicas y la creación de tecnología que sería el producto de acuerdo con el desarrollo de los capítulos anteriores involucrando incluso el aporte de recursos para este desarrollo.

Debido a que el comité de coordinación de seguimiento al sistema financiero puede verse afectado por ataques cibernéticos que afectarían el cumplimiento de sus objetivos comunes e incluso los estratégicos, la normatividad da la posibilidad de generar grupos de trabajo interinstitucional (Decreto 1954 de 2014) con el fin de desarrollar temas evitando afectaciones de esta índole.

Para el Fondo de Garantías de Instituciones Financieras (Fogafín), la aplicación de la Circular No 7 de la Superintendencia Financiera de Colombia (Colombia, 2018) debe ser adoptada con el propósito de mantener los requisitos mínimos para la gestión de la ciberseguridad; sin embargo, no aplica para las otras entidades de la red.

La aplicación de esta Circular deberá generar resultados en la gestión del riesgo en Ciberseguridad para Fogafín, que podrían ser implementados en el grupo de colaboración .

No existe una guía para la definición de medidas normativas que permitan adoptar el intercambio de información como parte de una gestión de incidentes cibernéticos; sin embargo, al revisar el convenio de Budapest (Europe, 2001), como un referente, la sugerencia se orienta en contemplar las sanciones y afianzar las jurisdicciones, este convenio desarrolla dentro de sus principios elementos a tener presente como la confidencialidad, la conservación de los datos almacenados y la asistencia mutua.

La definición de herramientas jurídicas para el proyecto busca fortalecer los compromisos y establecer los lineamientos para el desarrollo de este. La normatividad que se genere deberá tener presente los capítulos anteriores permitiendo el desarrollo de cada uno de estos.

De acuerdo con lo anterior se creará una orientación y una base de los elementos que deben ser contemplados para el desarrollo de un convenio que permita la colaboración en el

marco del comité de coordinación de seguridad del sistema financiero y que además permite el desarrollo de AmeComp.

Este sistema busca ser un modelo de capacidades para la entidad que forme parte, permitiendo de forma directa o indirecta hacer parte en la detección, protección, respuesta y recuperación en incidentes cibernéticos.

Los atacantes mantienen el desarrollo continuo de sus capacidades y habilidades, dinamizando y optimizando sus métodos, es decir aumentando sus habilidades las cuales puede ofrecer como servicios especializados pese a ser considerado como un delito cibernético.

El resultado posterior a los análisis de la información recibida debe ser compartida con las unidades especializadas, que tienen como responsabilidad atender los incidentes de ciberseguridad como el CERT Nacional - Colcert (Computer Emergency Response Team), de forma inicial y posteriormente a los CERT del sector si existen, esto con el propósito de replicar la información, descartar falsos positivos en el reporte de incidentes cibernéticos o identificar otros componentes o elementos que pueden ser amenazas.

El desarrollo de este proceso implica un intercambio de información, lo que debe ser formalizado mediante un convenio de participación, en el cual la entidad que se adhiere a la red se compromete a cumplir los lineamientos definidos en pro de tener alertas y alarmas para evitar afectaciones en la infraestructura tecnológica de su entidad. Este convenio debe tener aceptación

de las partes y cumplir con los requisitos legales exigidos por la ley hoy día respecto a la clasificación de la información.

Además, este convenio debe solicitar la participación activa, el cumplimiento de los procesos definidos para el intercambio de información, la implementación de las herramientas tecnológicas, él envió del catálogo de activos susceptibles; como también las sanciones por el incumplimiento de todas estas acciones no realizadas de acuerdo con lo definido.

Se busca implementar esta herramienta como una capa de seguridad en la entidad, favoreciendo a todas las entidades que hacen parte de la solución, por tal razón debe ser retroalimentada constantemente con los resultados de las alertas reportadas, del uso de la información obtenida en cada uno de los tipos de inteligencia que se desarrollen (estratégica, operativa, táctica o técnica), permitiendo ajustar el sistema de forma constante el mismo sistema. Esta información debe permitir identificar la efectividad respecto a la solución de forma global.

De acuerdo con todo lo anteriormente descrito en el presente capitulo, se definen las siguientes políticas como base de la legislación a desarrollar:

Políticas:

Para ser parte de la red de colaboración, las entidades deben tener presente la generación de los siguientes lineamientos de acuerdo con el tipo de entidad y sector al que pertenece:

Las entidades deben firmar un convenio con el propósito de comprometerse a compartir la información correspondiente a los eventos o incidentes a los que han sido expuestos al momento en el que se presente. Este acuerdo debe contemplar la normatividad vigente respecto al tipo de información y además debe contemplar que la contraparte mantendrá de forma anónima el registro respecto a los detalles de la entidad que realizo el reporte.

La entidad que será parte debe remitir el listado de sus activos en el formato definido, esto para los fines respectivos de identificación de elementos que pueden ser afectados.

La entidad debe identificar sus riesgos de negocio (estratégico), que deben estar asociados a los riesgos cibernético por afectación tecnológica sobre los activos reportados.

El nodo central debe enviar las alarmas respectivas cada vez que obtenga nuevos indicadores de compromiso, reportado por alguna de los miembros de la red.

El nodo central debe mantener el anonimato de la entidad que realiza el reporte del evento o incidente, tomando únicamente como información de entrada el sector al que pertenece de la entidad que realizan el reporte y el dato del reporte.

Las entidades deben participar de forma activa, realizar los reportes de los diversos eventos o incidentes en ciber, una vez controlados o contenidos en la gestión de incidentes propia de la entidad.

El nodo central, debe realizar el análisis de los datos reportados mediante al apoyo de autoridades en búsqueda de posibles comportamientos que puedan afectar activos de otras entidades que pueden ser víctimas de estos mismos ataques.

El nodo central debe generar alarmas lo antes posible sobre todas las entidades que tienen activos comunes o relacionados con los activos afectados o atacados por la entidad que realizo el reporte.

Una vez reciba las alarmas las entidades, estas deben realizar las acciones respectivas que impidan la afectación en caso de que el ataque se propague a estas entidades.

Las entidades deben compartir mecanismos de protección realizados con el fin de mitigar o evitar el ataque de tal forma que sea aplicado por otras entidades.

En caso de no tener aplicabilidad la alarma generada o no exista alguna relación con sus activos, la entidad debe reportar a la central de procesamiento el falso positivo.

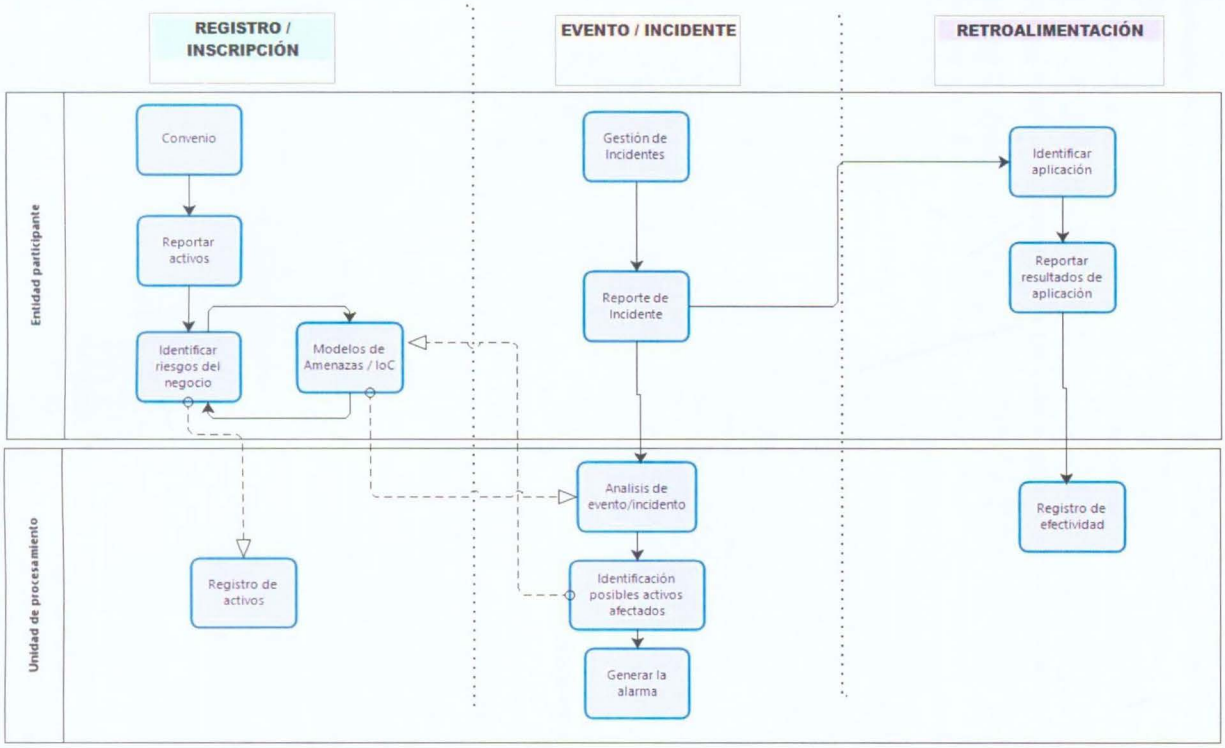

Ilustración 11 Proceso descriptivo de lineamientos a definir

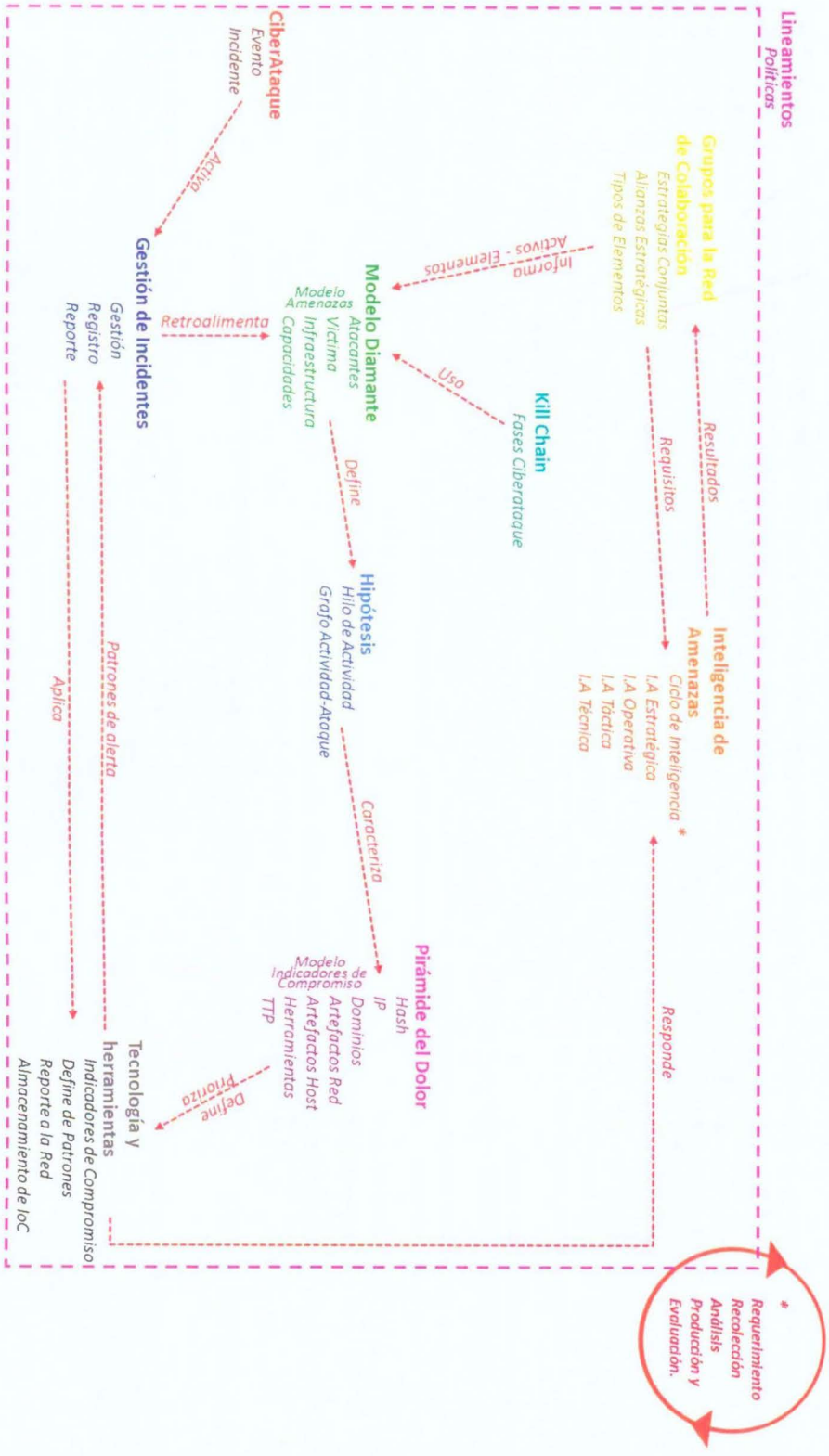

Ilustración 12 Esquema General "AmeComp"

Conclusiones

La participación de las entidades como miembro de la red de colaboración, permite sumar sus capacidades fortaleciendo sus defensas ante los cibercriminales.

Existe herramientas tecnológicas que permiten la implementación del proyecto, sin incurrir en costos elevados; sin embargo, se requieren recursos para la implementación, la gestión y mantenimiento.

El propósito de generar colaboración no solo busca tener la participación de quienes hacen parte del grupo, sino que, además, permite tener mayor cantidad de datos que pueden confirmar o ratificar eventos o incidentes comunes e incluso el analizar esta información de forma colectiva.

Existen diferentes métodos, guías y proyectos que permiten compartir y analizar los datos asociados a eventos o incidentes cibernéticos, cada uno de estos tienen elementos favorables lo que indica que deben ser analizados y evaluar las características apropiadas con el propósito de cumplir con el objetivo del proyecto.

La evolución de ataques y el desarrollo de amenazas cibernéticas de manera globalizada, genera la necesidad de implementar soluciones globales igualmente lo que implica tener información oportuna, efectiva y real que permita contrarrestar estos eventos.

Cada miembro debe ser consiente del papel que representa como miembro de la red identificado el valor que obtiene y que genera al recibir y compartir información.

Se deben definir herramientas jurídicas que definan e incentiven la participación de las partes, fortaleciendo los acuerdos de colaboración que se generen.

El aumento de participantes en una implementación del AmeComp con un alcance mayor, permitiría tener más información que apoyaría a las estrategias para contrarrestar la ciberdelincuencia en el país.

Bibliografía

Mandian Corporation, (2013), Openioc, http://www.openioc.org/

Veris Community, (2016), Veris, http://veriscommunity.net/

The Mitre Corporation, (2016), Cyber Observable eXpression (CybOX™), http://cyboxproject.github.io/

R. Danyliw, (2009), Incident object description and exchange format, https://www.ietf.org/rfc/rfc5070.txt

The Mitre Corporation, (2016), Trusted Automated eXchange of Indicator Information (TAXII™), http://taxiiproject.github.io/

The Mitre Corporation, (2016), Structured Threat Information eXpression (STIX™), https://stixproject.github.io/

Department of Homeland Security, (2016), Traffic Light Protocol (TLP) Definitions and Usage, https://www.us-cert.gov/tlp

AlienVault, Inc,(2016), AlienVault Open Threat Exchange, https://www.alienvault.com/open-threat-exchange

GitHub, Inc,(2016), Collective Intelligence Framework, http://csirtgadgets.org/

NATO Science for Peace and Security Series - D: Information and Communication Security : Best Practices in Computer Network Defense : Incident Detection and Response. (2014). Burke, NL: IOS Press.

David Chismon y Martyn Ruksya Ltd, M. I. (2015). Threat Intelligence: Collecting, Analysing, Evaluating Centre for the Protection of National Infraestructure.

Nacional, M. d. D. (2009). Ciberseguridad y Ciberdefensa: Una primera aproximación. Nota de investigación 03. Retrieved from https://www.mindefensa.gov.co/irj/go/km/docs/Mindefensa/Documentos/descargas/estudios%20sectoriales/Notas%20de%20Investigacion/Ciberseguridad%20y%20ciberdefensa.pdf

Hun-Ya Lock. (2013). Using IOC (Indicators of Compromise) in Malware Forensics

Open IoC. Sophisticated Indicators for the Modern Threat Landscape: An Introduction to OpenIOC

Society, O.-A. O. S. f. t. I. (2016). Cyber Threat Intelligence (CTI) TC. Retrieved from https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti

Referencias Bibliográficas

Abawajy, J. H., Mukherjea, S., Thampi, S. M., & Ruiz-Martínez, A. (2015). *Security in Computing and Communications: Third International Symposium, SSCC 2015, Kochi, India, August 10-13, 2015. Proceedings*: Springer International Publishing.

Andreeski, C., Baraković Husić, J., Baraković, S., Baykal, N., Ben-Israel, G. M., Bogdanoski, M., . . . Vaseashta, A. (2014). NATO Science for Peace and Security Series - D: Information and Communication Security : Cyber Security and Resiliency Policy Framework. In. Burke, NL: IOS Press.

Bianco, D. (2013). The Pyramid of Pain. Retrieved from http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html?m=1

Bluecloud. (2014). IOC-EDT. Retrieved from http://bluecloudws.github.io/ioceditor/

Candau, J. (2017). Ciberinteligencia, complemento para la ciberseguridad. *Red de Seguridad,* 6.

Circular Externa 7 de 2018

Instrucciones relacionadas con los requerimientos mínimos para la gestión del riesgo de ciberseguridad, (2018).

Dalziel, H. (2015). How to Define and Build an Effective Cyber Threat Intelligence Capability. In: Elsevier.

Europe, C. o. (2001). *Convenio sobre la Ciberdelincuencia*. Budapest

Focus, M. (2017). Log Events Reference Guide. Retrieved from https://community.saas.hpe.com/t5/Syslog/Dell-SonicWall-SONICOS-5-9-6-0-5-6-2-Log-Events-Reference-Guide/td-p/1587224

Galindo López, C. M. (2014). La Firma Electrónica Avanzada y su Certificación. *Revista de la segunda Cohorte del doctorado en seguridad estrategica,* 110.

Hutchins, E. M., Clopperty, M. J., & Amin, R. M.). *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*. Lockheed Martin Corporation.

ICONTEC. (2006). Norma Técnica Colombiana NTC-ISO/IEC 27001. In *Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI)*.

Inc., D. (2014). *Log Events Reference Guide with Enhanced Logging*. In D. I. SonicWALL (Ed.).

Legislativo, O. (2009). Inteligencia y Contrainteligencia. In: Instituto de Ciencia Política Hernan Echevarria Olózaga.

Ltd, M. I. (2015). Threat Intelligence: Collecting, Analysing, Evaluating In: Centre for the Protection of National Infraestructure.

Martin, L. (2015). Gaining the Advantage. In: Lockheed Martin Corporation.

Nacional, C. C. (2015). GUÍA DE SEGURIDAD (CCN-STIC-425) Ciclo de Inteligencia y Análisis de Intrusiones. In. España: Centro Criptológico Nacional.

Decreto 393, (1991).

Ley 795, (2003).

Decreto 1954, (2014).

República, B. d. l. (2015). Sectores económicos.

Romero, C., Berger, G., Ickis, J. C., Lozano, G., Roitter, M., Pires, J. T., . . . https://publications.iadb.org/handle/11319/313#sthash.Jjz7JiSQ.dpuf, -. S. m. a. (2005). Alianzas Sociales en América Latina: Enseñanzas Extraídas de Colaboraciones Entre el Sector Privado y Organizaciones de la Sociedad Civil. In. Washington, US: Inter-American Development Bank.

Torres, C. E. T. (2014). Inteligencia colectiva: enfoque para el análisis de redes/Swarm intelligence: approach to the analysis of networks/Inteligência colectiva: abordagem para a análise de redes. *Estudios Gerenciales, 30*(132), 259-266.

Trejo Medina, D. (2013). Inteligencia Colectiva. In: DanTM.

Villalón, A. (2016). Amenazas Persistentes Avanzadas. In: Nau Llibres.

Wong, V. M. M., & González, R. M. (2008). *Modelo de implementación y operación de un Security Operation Center a partir de sus procesos específicos y basando en ITIL.*