Ciberdefensa Abierta: El Ciclo de la Inteligencia de Amenazas con Software Libre

Lozano, Eduard.
edlozanoa@udistrital.edu.co
Universidad Distrital Francisco José de Caldas

Resumen— Este artículo establece las pautas fundamentales para la adopción de proyectos provenientes de comunidades de software libre en entornos empresariales, con énfasis en su aplicación en sistemas de seguridad informática. Se busca visibilizar el potencial de estas soluciones para construir ecosistemas seguros, legítimos y escalables, capaces de integrar múltiples capas de protección e inteligencia contra amenazas.

Se analiza el impacto estratégico del software libre en la ciberdefensa moderna, abordando los alcances técnicos y legales asociados a las distintas licencias disponibles. Asimismo, se clarifican las diferencias entre software libre y software propietario, destacando que el acceso al código no implica necesariamente gratuidad ni ausencia de restricciones.

El artículo también categoriza los principales tipos de proyectos existentes en comunidades open source, evaluando sus capacidades para integrarse con estándares y normativas de seguridad empresarial. Esta aproximación busca fomentar la adopción informada de soluciones abiertas, promoviendo prácticas sostenibles y auditables en la gestión de riesgos digitales.

Índice de Términos— Seguridad de código abierto, Inteligencia de amenazas, SOC, Arquitectura distribuida de seguridad y SIEM (Gestión de Información y Eventos de Seguridad).

I. INTRODUCCIÓN

El panorama de las ciber amenazas está en un crecimiento en la sofisticación con las nuevas tecnologías si tomamos la metodología PESTEL como referencia para determinar las tendencias futuras se deben ver las diferentes vulnerabilidades y oportunidades que los actores maliciosos y organizaciones criminales pueden usar para explotar y generar ataques utilizando Tácticas, Técnicas y Procedimientos (TTPs) más especializados haciendo que la defensa reactiva tradicional sea insuficiente para prevenir estas fallas [1]. En este contexto, la inteligencia de ciberamenazas (CTI) se vuelve un pilar fundamental en la ciberdefensa proactiva y la predictiva [2]. La CTI permite a las organizaciones comprender el panorama de amenazas, anticipar movimientos adversarios y tomar decisiones informadas para mitigar riesgos. Sin embargo, la implementación efectiva de programas de CTI a menudo depende de plataformas comerciales (Threat Intelligence Platforms - TIPs) cuyos costos de licenciamiento, implementación y mantenimiento representan una barrera económica significativa, especialmente para Pequeñas y Medianas Empresas (PYMES), instituciones académicas y organizaciones en el sector público [3].

Los ecosistemas de software libre (Free and Open-Source Software - FOSS) es una alternativa emergente que presenta un valor representativo en la estrategia y viabilidad en la democratización de acceso a capacidades de CTI avanzada. Existen proyectos FOSS como MISP (Malware Information Sharing Platform) que se han consolidado como un referente de estándar para el intercambio de Indicadores de Compromiso (IoC) mediante la creación de comunidades de confianza [4]. Plataformas más recientes como OpenCTI permiten el acceso la visualización y organización de amenazas alineándose a estándares como STIX/TAXII para el modelado e intercambio de IoCs TTPs y actores de amenaza [5]. Los FOSS no solo reduce drásticamente los costos, sino que también ofrece una transparencia, flexibilidad y capacidad de personalización inalcanzables en soluciones propietarias, fomentando una innovación impulsada por la comunidad global.

El objetivo principal de este artículo dar las bases para que se diseñe, implemente y valide una arquitectura funcional y de bajo costo para gestionar el ciclo de vida completo de la inteligencia de amenazas utilizando exclusivamente herramientas de software libre. Para alcanzar este objetivo, se han establecido las siguientes metas específicas: 1) Analizar las capacidades de herramientas de código abierto como componentes centrales de la arquitectura; 2) Explicar el ciclo de vida que detalle el flujo de datos desde la recolección de fuentes OSINT (Inteligencia de Fuentes Abiertas) hasta la gestión de un caso de respuesta a incidentes; y 3) Justificar el uso de metodología estructurada para la gestión de seguridad de una organización.

Este artículo se estructura de la siguiente manera: la investigación de los aspectos más relevantes del CTI detallando el ciclo de vida de la inteligencia de amenazas y revisando trabajos relacionados en el campo. Describe la funcionalidad y características de las herramientas OSS y su relevancia con el CTI. Exponer la arquitectura de proyectos Open Source para un ecosistema de CIT. Los resultados obtenidos de la encuetas con los datos para justificar la investigación y validar su eficacia en la práctica. Finalmente, la conclusión sobre el resultado de la investigación como la justificación de la adopción de metodologías estructuradas para la gestión de la seguridad en una organización.

II. CICLO DE VIDA DE LA INTELIGENCIA DE AMENAZAS

A. Inteligencia de Amenazas

La Inteligencia de Amenazas es un campo de la ciberseguridad centrado en el análisis y procesamiento de información. La Ciberinteligencia de amenazas (CTI) recopila, filtra y analiza información de amenazas o incidentes que pueden afectar a una organización, también busca determinar las motivaciones, capacidades y la infraestructura que utilizan los actores maliciosos. No se trata simplemente de una lista de indicadores técnicos, como direcciones IP o hashes de programas maliciosos, sino de un conocimiento contextualizado y predictivo que permite a una organización pasar de una postura de seguridad reactiva a una proactiva. Según Gartner, la inteligencia de amenazas es "conocimiento basado en evidencia, incluyendo contexto, mecanismos, indicadores, implicaciones y asesoramiento accionable, sobre una amenaza o peligro existente o emergente para los activos" [6]. Esto se logra por medio de la recopilación de fuentes sobre amenazas (TIF) que pueden ser de dos tipos, las externas que van desde organizaciones públicas y privadas que se encargan de concentrar y compartir esta información a las partes interesadas sobre las nuevas amenazas globales, y las fuentes internas que va en la recolección de información de los sistemas a partir de logs, alertas de SIEM (Sistema de Gestión de Eventos e Información de Seguridad), y de más sistemas de control y seguridad que se tengan implementados.

Esta información permite a las organizaciones y personal responsable la toma de decisiones, desde analistas técnicos hasta el nivel estratégico, anticipar las Tácticas, Técnicas y Procedimientos (TTPs) de los actores de amenaza, fortalecer sus defensas de manera informada y responder a los incidentes con mayor eficacia.

Tipos de inteligencia de amenazas

La Inteligencia de amenazas se clasifica en tres niveles distintos el cual varía según su audiencia y aplicación: Inteligencia estratégica, Inteligencia táctica e Inteligencia estratégica.

La **inteligencia de amenazas estratégica** tiene como objetivo a la alta dirección y a los responsables de toma decisiones donde se entregan análisis y métricas sobre el panorama de los riesgos, las motivaciones de los actores de amenazas y el posible impacto en la operación de la organización ayudando en la toma a la toma decisiones sobre inversión en mecanismos de seguridad y en la aplicación de política organizacionales para contra restar estas amenazas [7].

La **inteligencia de amenazas táctica** tiene un enfoque más a las Tácticas, Técnicas y Procedimientos (TTPs) de los actores de las amenazas y tiene como destino a los profesionales de seguridad y su objetivo es proporcionar un contexto sobre "como" atacan los actores para que de esta manera se puedan mejorar los controles defensivos y mejorar las estrategias de detección para mitigar las amenazas que amenacen la organización [8]. El modelo de diamante y el marco MITRE ATT&CK [9] para el análisis de intrusiones son las más utilizadas las cuales buscan detallar y analizar los TTP, a lo largo del documento se profundizará sobre estos y analizará su uso y aplicación en entornos reales y organizados.

La **inteligencia de amenazas operacional** se enfoca en los detalles técnicos e inmediatos de un ataque en curso o inminente. Esta es la inteligencia utilizada en el día a día por los equipos de respuesta a incidentes y como los analistas de la seguridad. Su contenido principal son los Indicadores de Compromiso (IoCs), que son las huellas digitales de una actividad maliciosa, tales como direcciones IP, dominios de mando y control (C2), o hashes de malware [10]. El análisis de estos indicadores permite no solo detectar y bloquear amenazas activas, sino también identificar los vectores de ataque más característicos y reconstruir los patrones de comportamiento del adversario durante una intrusión.

B. Ciclo de vida de la inteligencia de Amenazas aplicado al Ciber inteligencia

El **Ciclo de Vida de la Inteligencia de Amenazas** es un modelo que es ampliamente aceptado en la industria y la academia, es utilizado y adaptado en diversos campos como gobierno, defensa, sector salud y energía e infraestructuras críticas, en el campo de la tecnología y telecomunicación segmenta el proceso de CTI en seis fases lógicas e interconectadas que transforman datos brutos en inteligencia accionable [12]. Este ciclo no es un proceso lineal, sino un bucle continuo de mejora y refinamiento.

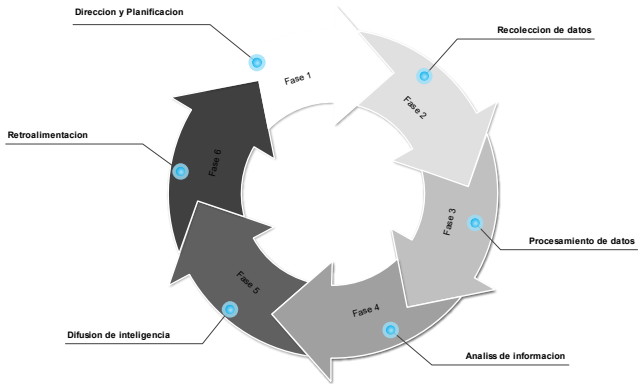


Fig. 1 Ciclo de vida CTI (Adaptada) [13][14]

Fase 1: Dirección y planificación

Esta fase es la inicial la cual su enfoque está en definir los alcances y objetivos de nuestro programa de CTI. Estable los requisitos de inteligencia basados en los activos críticos de la organización y el panorama de amenazas relevantes según nuestro sector.

Se deben definir los Requisitos Prioritarios de Inteligencia (PIRs) que guiara las preguntas para el programa de ciber inteligencia de nuestra organización, estos PIRs se aplican a los

tipos de inteligencia estableciendo los objetivos específicos a las preguntas por tipo:

PIR Estratégico (Para la dirección y responsables de toma de decisión): Las preguntas que se orientan en este nivel se dan bajo el contexto de la organización, los objetivos y proyecciones a futuro, estas preguntas le dan a la dirección la oportunidad de evaluar los objetivos de la organización con respecto al tratamiento de amenazas y la definición de un presupuesto en base a los objetivos no limitándose a proteger solo la infraestructura tecnológica sino también a proteger el concepto del negocio [27].

En los PIR Estratégicos aplicados en el CTI están divididos en cuatro conceptos de la gestión corporativa y del análisis de riesgos:

- **Protección de Activos Críticos:** Clasificar los activos de la información por su impacto donde se evalué el mayor daño a la viabilidad financiera o ventaja competitiva. Un ejemplo del tipo de pregunta es:
  ¿Qué activo de la información causaría un mayor daño al ser vulnerado, robado o alterado?

  ¿Qué proceso del negocio es tan critico que su interrupción por más de 24 horas pondría el riesgo la continuidad de la empresa?

  ¿Qué información o propiedad intelectual nos diferencia de nuestros competidores?

- **Riesgos en la reputación o marca:** De acuerdo con el contexto organizacional la reputación y visibilidad de la marca en el mercado se puede ver afectado por diferentes eventos de seguridad informática que pueden comprometer la confianza del público o asociados. Un ejemplo del tipo de pregunta es:
  ¿Qué tipo de incidentes en seguridad causaría un mayor impacto en la pérdida de confianza?

  ¿Qué actores de amenazas (hacktivistas) podrían tener motivaciones específicas según el contexto de nuestra organización que puedan generar campañas de desinformación y desprestigio?

- **Proyecciones crecimiento y nuevos servicios:** Con el constante desarrollo de nuevas líneas de negocio o servicios nuevos crecen los diferentes riesgos de seguridad que pueden afectar las nuevas operaciones por lo que se debe planificar desde un inicio los objetivos de seguridad proyectados al largo plazo de su implementación. Un ejemplo del tipo de pregunta es:
  ¿Qué nuevos riesgos cibernéticos se están asumiendo que antes no existían?

  Si el crecimiento está dado en nuevos mercados internacionales: ¿Qué riesgos en la geopolítica de la zona o el país representa una amenaza cibernética para nuestra infraestructura y asociados (Empleados)?

- **Continuidad del Negocio:** Se debe evaluar la ubicación de los activos de la información y garantizar su confidencialidad, integridad y disponibilidad para que la operación no sea interrumpida por un evento que comprometa los servicios o que su recuperación no afecte la operación por un periodo de tiempo prolongado. Un ejemplo del tipo de pregunta es:
  ¿Cuál es el impacto de depender de un único proveedor de tecnología o servicio?

  ¿Cuál es la amenaza externa con mayor potencial en interrumpir la operación?

Las preguntas o conceptos en los PIR estratégicos pueden variar según la organización por lo que depende de cada negocio estructurar y organizar el esquema que se ajuste a su operación y negocio.

PIR Táctico (Para los equipos de seguridad): Definidos los requisitos prioritarios de inteligencia (PIR) por los directivos los equipos de seguridad deben establecer los mecanismos para la prevención, detección y corrección para los objetivos de seguridad requeridos, estos deben ajustarse según los alcances y presupuestos definidos por la dirección, un mal dimensionamiento de los PIR Estratégicos pueden llevar a un mal diseño de presupuesto y generar brechas de seguridad no deseadas.

La pregunta orientadora es el "como" cumplir con los objetivos de seguridad planteados. Para el PIR Táctico aplicado en el CTI se puede dividir en tres mecanismos o niveles de seguridad:

- **Prevención:** Se deben definir los principales vectores de ataque, tácticas y vulnerabilidades de los activos de la información y aplicaciones. Un ejemplo del tipo de pregunta es:
  ¿Cuáles son los vectores de ataque son más exitosos para el contexto de nuestra industria?

  ¿Qué tácticas de ingeniería social son más exitosas para engañar a nuestros colaboradores?

- **Detección:** Se busca establecer mecanismos para la detección temprana de amenazas con el fin de mitigar el riesgo de exposición y crecimiento de un actor dentro de la organización. Un ejemplo del tipo de pregunta es:
  ¿Cuáles son las técnicas de movimiento o estalación lateral son más utilizadas por los actores de amenazas aplicada a nuestro entorno?

  ¿Qué herramientas de software "legitimo" están siendo utilizados por los atacantes para evadir la detección?

- **Respuesta:** Se deben aclarar las técnicas utilizadas por los actores maliciosos para establecer las respuestas adecuadas. Un ejemplo del tipo de pregunta es:
  ¿Qué técnicas son más utilizadas para la extracción de información?

¿Cómo han evolucionado las TTPs de los principales actores maliciosos que afecten a nuestro sector?

Estas preguntas ayudan a estructurar y contemplar los mecanismos que se debe usar para el tratamiento de amenazas.

PIR operacional (Para los centros de operaciones): Los requisitos prioritarios de inteligencia en la operación están dados a estar actualizados sobre los IoC técnicos y observables que actualmente se encuentran más utilizados y realizar las respectivas restricciones en las herramientas de seguridad de la organización.

La pregunta que orienta es el "que" y el "donde" para detectar y bloquear las amenazas activas, se deben definir tres niveles guía para establecer los PIRs Operacionales:

- **Triaje y Clasificación de alertas:** Se deben clasificar el nivel de amenaza para los eventos de seguridad para esto se debe realizar una clasificación y priorización de los activos de información basado en los PIRs Estratégicos. Un ejemplo del tipo de pregunta es:
  ¿Qué herramientas nos permiten detectar rápidamente actividades relacionadas con anomalías de la operación?

  ¿Qué patrones comunes en los logs son indicadores de un ataque?

- **Caza de amenazas:** Se debe saber dónde buscar las amenazas comunes y analizar los patrones de conexión para determinar anomalías dentro de la operación habitual. Un ejemplo del tipo de pregunta es:
  ¿Qué indicadores de compromiso (dirección IP, Dominios o Has de archivos) están asociados a campañas de malware o phishing están activas en este momento?

  ¿Qué conexiones de red saliente desde servidores que normalmente no consulten fuentes externas podrían ser un indicador de exfiltración de datos?

Los requisitos de prioridad de inteligencia definen y enfocan la operación del CTI, como cada organización tiene una estructura operacional, requisitos de operación y se aplican a sectores diferentes las preguntas y guías pueden variar, pero es importante estructurarlas para generar una buena planificación y dirección. Se debe tener en cuenta que las definiciones de inteligencias son ampliamente utilizadas en diversos campos no solo orientados a riesgos cibernéticos por lo que es importante generar una extracción general de los conceptos de inteligencia y aplicarlos al campo de acción de la ciber inteligencia.

Otras maneras en la que se puede estructurar es con una metodología PESTEL la que se puede usar para dimensionar las posibles amenazas y anticiparnos a estas en nuestra fase de planificación se debe tener las siguientes consideraciones [1]:

- **Político:** Limitación de acceso a recursos digitales por leyes y restricciones y ciber poder de las potencias globales.
- **Económico:** Ciberataques, incremento en impuestos y fluctuaciones en monedas digitales (Incentivo de los atacantes).
- **Social:** Afectaciones de la imagen y reputación a la exposición a ataques y desprestigio en redes sociales y alto crecimiento de grupos de cibercrimen.
- **Tecnológico:** Mayor vectores de ataque, mayor densidad de dispositivos y vulnerabilidad digital.
- **Ecológico:** Considera la seguridad de las infraestructuras críticas (energía, agua), el impacto de desastres naturales en la continuidad del negocio y la ciberseguridad de los sistemas de control industrial (ICS/SCADA)
- **Legal:** Nuevas leyes de protección de datos y ciberdelincuencia (como GDPR), las regulaciones de notificación de brechas y los requisitos de cumplimiento de su operación.

Fase 2: Recolección de datos

Una vez aclarado el alcance y los objetivos vamos a usar cuatro tipos de disciplinas de inteligencia:

- **OSINT (Inteligencia de Fuentes Abiertas):** Fuentes de amenazas públicas, blogs de seguridad, redes sociales y repositorios de código.
- **HUMINT (Inteligencia de Fuentes Humanas):** Información en foros, grupos, seminarios y comunidades o interacciones humanas entre especialistas del ámbito privado y público.
- **TECHINT (Inteligencia de desarrollos tecnológicos):** Datos de analistas de malware e infraestructura de tipo honeypot (Señuelos) para recolección de datos en tiempo real de ataques para la recolección de datos como riegos, vectores de ataque y evidencias de ataques.
- **GEOINT (Inteligencia de Fuente Geoespacial):** Fuente de datos para determinar información de ubicación y tendencias de ataques referido a geolocalización.

Existentes otras disciplinas de inteligencia aplicadas a otros campos que si bien no son tan utilizadas en el CTI siguen siendo fuentes de apoyo.

TABLA I
DISPLINAS DE INTELIGENCIA [6]

SIGLAS	DESCRIPCIONES
COMINT	Inteligencia de Comunicaciones
CULTINT	Inteligencia Cultural
DFINT	Inteligencia Forense Digital
ELINT	Inteligencia Electrónica
GEOINT	Inteligencia Geoespacial
HUMINT	Inteligencia de Fuentes Humanas
IMINT	Inteligencia de Imágenes
MARKINT	Inteligencia de Mercados
MASINT	Inteligencia de Medidas y Firmas
SIGINT	Inteligencia de Señales
SOCMINT	Inteligencia de Redes Sociales
TECHINT	Inteligencia Técnica
TELINT	Inteligencia de Telemetría

Fase 3: Procesamiento de datos

En la fase de procesamiento de datos es donde converge la información de datos brutos (datos sin procesar) y se transforman en un formato compresible y útil para el análisis. Esta fase es indispensable para realizar el puente entre la recolección de los datos y la aplicación de inteligencia accionable sobre esta información. Las actividades de esta fase se incluye el proceso de decodificar, traducir y filtrar para reducir los datos que pueden ser irrelevantes o pueden estar duplicados, de esta manera organizarla de manera estructurada.

El objetivo final del procesamiento no es analizar la información, sino prepararla y refinarla para que los analistas puedan trabajar de manera eficiente en la siguiente fase de Análisis de información [16].

El procesamiento de datos de rige por un flujo de trabajo lógico diseñado para transformar los datos brutos en información organizada y lista para el análisis, este flujo es una secuencia de pasos lógicos que consiste en las mejores prácticas de la industria para estructurarlos.

- **Ingestión y normalización:** Una vez los datos son recopilados de múltiples fuentes inmediatamente se someten a un proceso de normalización que consiste en convertir los datos a un formato común, esto incluye la estandarización de los campos como las fechas, nomenclatura de las fuentes y convertir distintos formatos de logs a un esquema único. Para esto se usan estándares facto que son ampliamente usados como el CEF (Formato Común de Eventos - Common Event Format) que estructura la información de logs para facilitar su manejo automático [17].
- **Filtrado y reducción:** Este paso elimina lo que se cataloga como “ruido”, es decir, descartar los datos corruptos, duplicados o que carezcan de calidad y valor para la investigación. El objetivo de este paso es enforcar los recursos del análisis exclusivamente a los datos que definimos como pertinentes en nuestra Fase de dirección y planificación. Se pueden crear filtros basados en listas blancas que pueden filtrar los datos de manera automática tanto de las fuentes como de la información relevante que especifiquemos [18].
- **Enriquecimiento y Correlación:** Este paso busca ampliar el valor de la información recolectada sobre los eventos generados dado que los datos que se entregan contienen información únicamente de las fuentes se pueden ampliar por medio de utilizar una capa de contextualización de los datos y enriquecer la información. Un ejemplo de este paso es la validación de las direcciones IP de origen que generan un evento, solo este valor nos da poca información, pero se pueden correlacionar las direcciones IP con fuentes de geolocalización, revisando al propietario del ASN (Número de Sistema Autónomo), el historial de la reputación en servicios de RBL (Lista de Bloqueos en Tiempo Real) y una resolución inversa de DNS para tener más información.

  La correlación se aplica a todos los campos que se pueden relacionar y pueden ser comparados con otras fuentes externas o bases de datos globales delimitadas en la fase dos de recolección de datos con el fin de enriquecer la información, una lista de los campos comunes que se pueden validar son direcciones ip, dominios, direcciones de correo, hash de documentos o aplicaciones, entre otros datos que se pueden obtener y relacionar con los logs según las fuentes [19].

- **Estructuración y modelado:** Es el paso final del procesamiento de los datos donde la información ya limpia, filtrada y enriquecida se organiza según el modelo de estandarización usado esto no solo facilita el análisis humano, sino que permite el procesamiento automático y el intercambio de inteligencia entre sistemas.
  La información se mapea de marcos de referencia reconocidos en la industria y aplicados según los objetivos del sistema:

  STIX/TAXII: Para un intercambio automatizado, los datos se convierten en objetos STIX (Structured Threat Information eXpression), que es el lenguaje estándar para describir la inteligencia de amenazas de forma estructurada [5] [20] [21].

  Los objetos mencionados en la Tabla II y Tabla III definen los objetos globales de la estructura esto se representa bajo formato JSON, cada objeto contiene datos y están estructurados con propiedades diferentes [20]. TAXII es el protocolo de aplicación que se usa para la comunicación de información sobre ciber amenazas de forma sencilla y estables funciona como una API RESful [21].

TABLA II
OBJETOS DE DOMINIO STIX (SDO) [20]

OBJETOS	DESCRIPCION
Patrón de ataque	Describe patrones de comportamiento adversario para comprometer objetivos.
Campaña	Agrupación de actividades o ataques maliciosos en un período de tiempo.
Curso de acción	Recomendación de acciones a tomar en respuesta a una amenaza.
Agrupamiento	Agrupación explícita de objetos STIX con un contexto compartido.
Identidad	Describe individuos, organizaciones o grupos reales.
Indicador	Patrón para detectar actividad cibernética sospechosa o maliciosa.
Infraestructura	Describe sistemas, servicios o recursos utilizados por un adversario.
Conjunto de intrusión	Conjunto de comportamientos y recursos adversarios con propiedades comunes.
Ubicación	Representa una ubicación geográfica.
Malware	Representa código malicioso utilizado por un adversario.
Análisis de malware	Metadatos y resultados de un análisis estático o dinámico de malware.
Nota	Proporciona contexto adicional y texto informativo a otros objetos STIX.
Datos observados	Hechos y entidades observados en un sistema o red.
Opinión	Evaluación de la exactitud de la información contenida en un objeto STIX.
Informe	Colección de inteligencia sobre una o más amenazas o temas relacionados.
Actor de amenazas	Individuos, grupos u organizaciones que actúan con intenciones maliciosas.
Herramienta	Software utilizado por actores de amenazas para ejecutar ataques.

TABLA III
OBJETOS DE RELACION (SRO) [20]

OBJETOS	DESCRIPCION
Relación	Vincula dos objetos STIX (SDO o SCO) para describir su nexo.
Observación	Denota la detección de un objeto STIX (como un indicador o malware) en un entorno real.

MITRE ATT&CK: Es un marco de trabajo que analiza el comportamiento del adversario que etiqueta las Tácticas, Técnicas y Procedimientos (TTPs) de los atacantes [9].

La interpretación del TTP según el modelo:

Tácticas (El "Porqué"): Representan el objetivo o la meta de alto nivel que un adversario intenta alcanzar en una fase específica del ataque. La matriz de MITRE ATT&CK define 14 tácticas las cuales se clasifican así: reconocimiento, desarrollo de recursos, acceso inicial, ejecución, persistencia, elevación de privilegios, evasión de defensas, acceso a credenciales, descubrimiento, movimiento lateral, recopilación, mando y control, filtración e impacto [23].

Técnicas (El "Como"): Este describe el método especifico que utiliza el adversario para lograr sus objetivos tácticos, cada táctica tiene múltiples técnicas. Actualmente la matriz define 211 técnicas distribuidas en las tácticas [23].

Procedimiento (El "Como exactamente"): Es la implementación particular de una técnica por parte del actor de la amenaza, una descripción más detallada y avanzada de la técnica utilizada. Actualmente la matriz define 468 sub técnicas que se distribuyen a las técnicas base [23].

Fase 4: Análisis de la información

La fase de análisis también llamada de producción es la etapa del ciclo de inteligencia donde la información ya procesada y estructurara se transforma en inteligencia. En este punto donde la intervención del juicio humano y las técnicas de analítica se usan para interpretar los datos, evaluar su fiabilidad y convertirlo en conocimiento accionable para responder a los requisitos de inteligencia y de esta manera tomar acciones preventivas y predictivas.

Los analistas buscan identificar los patrones, inferir las intenciones de los actores de la amenaza, predecir futuros vectores de ataque y evaluar el impacto potencial para la organización. Es llamado también "producción" ya que busca crear un producto final como resultado de la inteligencia como un informe, un indicador, una alerta o una presentación que comunicara a las partes interesadas información para la toma de decisiones [16]. Según el analista de la CIA, Richards J. Heuer, esta fase es susceptible a errores en el juicio por lo que el uso de Técnicas Analíticas Estructuradas (SATs) es fundamental para mitigar las preconcepciones y los sesgos cognitivos para asegurar la objetividad y el rigor del análisis [24]. El resultado no es simplemente una descripción de los hechos, sino una evaluación prospectiva que permite a la organización tomar decisiones informadas para reducir el riesgo.

Las técnicas de análisis estructurada (TAE - En ingles SAT) son métodos diseñados para reducir el riego de errores en el análisis de inteligencia este no se limita solo a la ciber inteligencia, sino que estas técnicas son ampliamente aplicadas a otros campos que requieren el análisis de datos. Su función principal es mitigar los sesgos cognitivos o atajos mentales que pueden llevar a conclusiones erróneas donde se asegura que los juicios se basen en una evaluación rigurosa y completa de evidencia.

Estas son tres agrupaciones de técnicas más utilizadas:

Técnicas de Diagnóstico: Esta técnica ayuda a los analistas que revisen los supuestos y sus conclusiones.

- **Revisión de Supuestos Clave (KAC):** Esta consiste en enumerar las suposiciones más importantes para su juicio y luego cuestionarse cada una, realizando preguntas sobre el porqué, considerar si su juicio o conclusión es erróneo

que pasaría. Esta técnica busca prevenir las conclusiones que no tengan una base sólida y que no pueda ser verificados [25].

- **Análisis de Calidad de la información (QOI):** Es una técnica que busca evaluar la veracidad y solides de las fuentes de información de la inteligencia donde se evalúa la integridad y la confiabilidad de los datos validando la evidencia que respalda el análisis, generando un sistema de calificación de las fuentes en función de su credibilidad y solidez de la información identificando posibles vacíos o datos que requieran más información que deba ser verificada. Esto asegura que el proceso de análisis tenga mayor respaldo en el juicio final con información fiable [25].
- **Análisis de Hipótesis en Competencia (ACH):** El objetivo de esta técnica no es buscar probar una hipótesis, sino que el analista busca identificar las posibles hipótesis y contrastarlas de manera simultánea contra los datos disponibles para que de esta manera refutar la hipótesis y al final tener menos inconsistencias en el análisis y tener un análisis más objetivo, esta técnica puede ser usada en un grupo de analistas para refutar sus propias hipótesis [25].

Técnicas de Desafío o Contraste: Estas técnicas buscan desafiar las interpretaciones y generar perspectivas alternativas.

- **Abogado del Diablo (Devil's Advocacy):** Consiste en asignar a un analista del equipo la tarea de criticar un análisis o plan de acción. Su trabajo consiste en encontrar las fallas, debilidades y supuesto errores en las conclusiones principales. Esta técnica busca que el equipo fortalezca su argumento y defienda su hipótesis de una manera más objetiva y estructurada [25].
- **"¿Qué pasaría sí?" (What If? Analysis):** Analiza desde una perspectiva un evento inesperado pero probable, explora las posibles consecuencias y desarrolla diferentes planes de contingencia para el posible impacto. Se puede interpretar con el siguiente ejemplo: "¿qué pasaría si un actor de amenaza desconocido publicara una vulnerabilidad de día cero?" con la idea del supuesto el analista puede tomar acciones preventivas a estos posibles eventos [25].

Técnicas de Previsión o Imaginativas: Estas técnicas buscan explorar futuros posibles y evitar los eventos inesperados que afecten la estrategia de la organización.

- **Análisis de Equipo Rojo (Red Team Analysis):** Esta técnica es realizada desde la perspectiva del atacante donde uno de los analistas busca simular ser el actor de la amenaza e intenta pensar y actuar como él lo haría, esto con el fin de anticipar sus movimientos, identificar las vulnerabilidades de los planes del actor y desafiar la suposición sobre la capacidad, escala e intención del atacante [25].
- **Pensamiento de Afuera hacia dentro (Outside-In Thinking):** Es una técnica que busca generar un nuevo enfoque cuando se enfrenta un problema inmediato donde es posible que ignoren otros factores o fuerzas del entorno que pueden influir en el resultado. Este método obliga al analista a analizar el contexto externo antes de centrarse en el actor o la situación específica [25].

Fase 5: Difusión de la información

La fase de difusión o diseminación es la tapa donde el conocimiento ya analizado y producido es entregado a quienes necesitan para tomar decisiones. El objetivo no solo enviar la información sino hacerlo de la manera correcta, a las personas correctas y en el momento adecuado para que tengan el mayor impacto.

En este paso se deben tener en cuenta tres pasos:

Identificar la audiencia: Antes de comunicar la información es importante saber a quién se le está comunicando, la información que le comunicamos a los diferentes actores que participan en la operación como la dirección que están más en un contexto administrativo, los gerentes y arquitectos de seguridad que son un contexto más táctico y los analistas y equipos de respuesta a incidentes que pertenecen más al contexto operacional. La información debe ser presentada según su contexto ya que cada actor contribuye a la operación de manera diferente y las decisiones pueden ser influenciadas por estas [7].

Selección del Formato y Producto Adecuado: Una vez identificado la audiencia objetivo se debe pensar en la manera adecuada de presentar la información no es lo mismo entregar un informe a un personal técnico a una persona más administrativa [16].

- Para la audiencia de tipo estratégica o administrativa se suelen usar informes ejecutivos, presentaciones de alto nivel, indicadores de gestión centrados en el riesgo y el impacto en el negocio.
- Para la audiencia de tipo más táctico se presentan informes sobre los TTPs de los adversarios con un análisis de las campañas o perfiles de los actores de amenaza.
- Para la audiencia de tipo más operacional se envían alertas en tiempo real, fuente de indicadores de compromiso (IoCs) o informes técnicos detallados sobre malware.

Canal de Distribución y Oportunidad: El método y el momento de entrega son importantes como el contenido. Un evento critico que es enviado por un canal de poca visibilidad como el correo puede pasar desapercibido. Se deben establecer canales de comunicación efectivos para cada tipo de evento y audiencia para que la información llegue en el momento y relevancia adecuada.

- Los informes de rutina pueden ser distribuidos por correo electrónico, plataformas internas o repositorios de información donde puedan ser consultados como un histórico y control de avance del sistema.
- Las alertas urgentes o que requieren atención prioritaria deben usarse canales de comunicación más instantáneos como chats seguros, sistemas de incidencias internos como

una plataforma colaborativa de respuesta a incidentes como DFIR-IRIS [26].

Fase 6: Retroalimentación.

Esta fase en la mayoría de la documentación relacionada se define dentro de la fase 5 y no como una fase independiente, aunque su importancia es alta para el cierre del ciclo la defino como una fase adicional, esta fase tiene como rol la mejora continua y el dinamismo de la inteligencia.

La estructura del proceso de retroalimentación consta de tres pastes y su objetivo es la mejora de todo el ciclo y refinar la utilidad de la inteligencia generada.

Recopilación de la retroalimentación: Existen dos maneras de realizar esta recopilación con mecanismos activos y la otra con mecanismos pasivos. El mecanismo activo consiste en recolectar esta información por medio de la interacción directa a través de la opinión en encuestas de satisfacción, entrevistas con las partes interesadas o la inclusión de un método simple de calificación. El mecanismo pasivo es a través de métricas de uso como la interacción con los informes, clic en los enlaces, los indicadores de compro proporcionado por las herramientas de seguridad y la escala en la mitigación de amenazas [7].

Análisis de la retroalimentación: Una vez recopilada la retroalimentación esta debe ser analizada para extraer las conclusiones más significativas se busca identificar los patrones y tendencias del resultado de la inteligencia dentro del contexto de la calidad de la inteligencia generada y la calidad de la información difundida. Categorizar la retroalimentación basado en criterios clave como la relevancia, precisión, oportunidad y claridad del producto final de la inteligencia [16].

Integración en el Ciclo: Este paso es el más importante ya queda como resultado de acciones concretas que modifiquen y mejoren el ciclo de inteligencia. Los resultados del análisis se utilizan como una entrada directa para la Fase de dirección y planificación, si los informes estratégicos no son leídos por la alta dirección se deben revisar y ajustar aplicando los requisitos de inteligencia (PIRs) con esto se ajusta el ciclo y evolución para que cada vez sean más relevantes para la organización.

C. El Software libre y su integración al ciclo.

El concepto de software libre, impulsado por la Free Software Foundation (FSF) y el Proyecto GNU, se articula sobre cuatro derechos irrenunciables que se centran en la libertad del usuario sobre su programa, en lugar de su costo. Estas libertades son un requisito de licencia que, por extensión, establecen la base para una arquitectura de seguridad superior al modelo de código cerrado o propietario estas licencias se dividen en dos grupos: permisivas y copyleft.

Licencias Permisivas: Imponen condiciones mínimas lo que permite una gran libertad a los usuarios. Una característica principal de estas licencias es que puede ser integrado a proyectos cerrados sin que su uso en el proyecto obligue a adoptar la misma licencia esto lo hace popular en el ámbito comercial, en la actualidad gran parte de los proyectos de código cerrado usan proyectos de software libre como base de su operación [27].

- Licencia de MIT: Licencia mas abierta, solo requiere que se mantenga el aviso de copyright y el texto de la licencia en las copias del software.
- Licencia Apache 2.0 (ALv2): Define mas detalles que la MIT y proporciona una concesión explicita de derechos de patente de las contribuciones de los usuarios [28].
- Licencia BSD (Berkeley Software Distribution: Incluye una restricción que prohíbe el uso del nombre de los contribuidores originales para promocionar un trabajo derivado.
- Licencias Copyleft: Las licencias que utilizan la ley de derechos de autor para asegurar que las libertades del software se preserven en sus trabajos y derivados. Implica que cualquier software modificado o extendido debe ser distribuido bajo la misma licencia [29]. Esta se divide en dos niveles de licenciamiento el Strong Copyleft (fuerte) y Weak Copyleft (débil).
- Licencia Pública General de GNU (GPL)(Fuerte): Es la licencia más utilizada y estipula que cualquier programa que se distribuya y contenga código bajo la GPL debe en su totalidad ser licenciado bajo GPL.
- Licencia Pública General Reducida de GNU (LGPL)(Débil): Su enfoque está orientado en a las bibliotecas de software. Permite la integración dinámica de bibliotecas LGPL con otros proyectos propietarios sin que este deba adoptar la licencia, para modificaciones a la biblioteca si deben ser liberadas bajo LGPL.
- Licencia Pública de Mozilla (MPL 2.0) (Debil): Esta licencia opera a nivel de archivo. Exige que las modificaciones a archivos cubiertos bajo la MPL se compartan. Permite también que los archivos se combinen con proyectos más grandes que compartan otras licencias ya sean abiertas o propietarias.
  Existe una práctica que no se considera una licencia en la que se renuncian a los derechos de autor que es la CC0 CC0 (Creative Commons Zero) que permite a los creadores dedicar su obra para el dominio público mundial donde renuncia a todos los derechos de autor.

La importancia de conocer los tipos de licencia en el software libre ayuda tomar decisiones informadas sobre las herramientas que tenemos a nuestro alcance y el nivel de libertad que tenemos sobre su uso y aplicación para que de esta manera escoger el producto que se acomode más a nuestra necesidad y validar los cambios de licencia ya que puede influir negativamente a largo plazo si esta cambia de abierta a cerrada.

Las Cuatro Libertades del Software Libre (SL) son la base para una Inteligencia contra Amenazas (TI) más robusta, rápida y colaborativa, al permitir el acceso completo al objeto de

estudio (el código fuente) y facilitar la distribución inmediata de contramedidas y herramientas de seguridad.

Las libertades fundamentales del SL (Software libre) se alienan directamente con las fases del ciclo de vida de la inteligencia contra amenazas (Recolección, procesamiento, análisis y difusión).



Fig. 2 Cuatro Libertades (Adaptada) [30]

- Libertad 0 (Utilizar): La libertad de usar el programa como se desee, con cualquier propósito [30].
- Libertad 1 (Estudiar y modificar): La libertad de estudiar cómo funciona el programa y cambiarlo para que satisfaga las necesidades del usuario [31].
- Libertad 2 (Compartir): La libertad de redistribuir copias a terceros para ayudar a la comunidad [32].
- Libertad 3 (Distribuir mejoras): La libertad de distribuir copias de versiones modificadas a terceros, permitiendo que toda la comunidad se beneficie [32].

La libertad 1 (Estudiar y modificar) y la libertad 3 (Distribuir Mejoras) que definen el requerimiento de acceso al código fuente es un componente esencial para la parte más técnica de TI. Para el análisis de vulnerabilidades el acceso al código fuente permite realizar investigaciones de seguridad y realizar ingeniería inversa y análisis estático y dinámico directo sobre el software. Lo que es crucial para identificar bugs de día cero, comprender su explotabilidad y generar indicadores de compromiso (IoC) detallados.

La libertad 3 permite que cualquier centro de respuesta a incidentes o un centro de operaciones de seguridad (SOC) pueda acelerar el desarrollo de parches y distribuir de inmediato a la comunidad acelerando la fase de difusión de inteligencia a las partes interesadas. En el desarrollo de proyectos internos de software es importante generar una auditoria continua de los cambios de las dependencias de código abierto que se utilizan en el código con el fin de mitigar las vulnerabilidades y reducir los riesgos en la cadena de suministros de software.

La libertad 2 (Compartir) asociado a nuestra fase de difusión de inteligencia que está directamente asociada a la colaboración global, el intercambio de inteligencia se ve fomentada por esta libertad donde se da la creación de plataformas de inteligencia contra Amenazas de Código Abierto (OSINT) como MISP (Malware Information Sharing Platform) [4] la cual utiliza estándares abiertos que facilitan la sincronización de datos de amenazas entre organizaciones.

Esta libertad nos impulsa en la adopción de herramientas de seguridad y análisis de código abierto como SIEMs (Gestión de Información y Eventos de Seguridad), Sandboxes (Entornos de pruebas seguro) y herramientas de análisis forense democratizando su acceso.

La libertad 0 (Utilizar) garantiza que las organizaciones puedan utilizar el software para funciones especializadas de seguridad sin restricciones de licencias. Algunos softwares privados tienen una versión comunitaria abierta para su uso al público si bien sus funciones son limitadas con respecto a sus versiones privadas estas ofrecen en algunos casos los aspectos necesarios para cubrir una necesidad de seguridad puntual por lo que la adopción de estas herramientas se puede integrar con otras herramientas con el fin de consolidar una arquitectura de software para el sistemas de CTI.

La Inteligencia contra Amenazas depende de la información de calidad y la acción oportuna. El modelo de las Cuatro Libertades garantiza que el código subyacente de los sistemas pueda ser inspeccionado (Libertad 1), corregido (Libertad 3) y que las herramientas de análisis de seguridad se compartan ampliamente (Libertad 2), creando un ecosistema de seguridad colectiva más adaptable y resiliente que el modelo de código cerrado.

Una fuente de datos en que se puede usar en la fase de recolección de datos pueden ser software y técnicas para la detección de vulnerabilidades y análisis de prácticas de software no recomendadas. Dentro de los productos que se pueden integrar en el ciclo de vida de desarrollo seguro y ciclo de inteligencia contra amenazas que tiene una licencia LGPLv3 es SonarQube Comunity Edition que permite realizar un análisis de código de diferentes herramientas

III. ECOSISTEMA DE CTI CON SOFTWARE LIBRE

Un ecosistema de Ciber inteligencia de Amenazas (CTI) con software libres es una infraestructura para la gestión de ciclo de vida de la inteligencia es construida con herramientas de código abierto. Este enfoque permite a las organizaciones desarrollar CTI robustos y transparentes. Controlando cada fase del proceso sin depender de licencias de software propietario democratizando la adopción del ecosistema a todo tipo de organizaciones.

La Fase 1 correspondiente a la dirección y planificación da la apertura para definir las herramientas con un propósito especifico que se alienen a los PIRs definidos para cumplir los objetivos de seguridad establecidos y las estrategias para abordar cada amenaza según el contexto de la organización.

Cada producto de software libre a mencionar estará relacionado con una de las fases del ciclo de vida y se definirá su relevancia bajo este contexto, las herramientas sugeridas son las que en la actualidad tienen una mejor presencia dentro de las herramientas de software libre y no limitan su uso para este propósito, esto no constituye que estas no puedan ser reemplazadas con otras herramientas similares ya que el objetivo

es dar una referencia sobre el software libre y el ciclo de vida de inteligencia adicional según el contexto organizacional y la arquitectura funcional del ecosistema se pueden integrar más herramientas y soluciones ya sean abiertas o privadas según el contexto organizacional.

Uno de los riesgos con el uso de software libre es que estas pueden cambiar el tipo de licenciamiento o privatizar algunas funciones y sacar una versión de pago para poder acceder por lo que es importante validar las actualizaciones de las licencias y características avanzadas de cada herramienta de software libre a implementar, estos cambios de licenciamiento suele afectar solo versiones futuras a partir de la fecha de actualización por lo que el sistema sigue operando sobre la licencia actual hasta que se actualice a una nueva versión.

Fase de recolección de datos:

En esta fase se recopila información bruta (PLAIN o RAW) de diversas fuentes donde las herramientas OSINT (Inteligencia de Fuentes Abiertas) son fundamentales.

En este contexto definimos cuatro disciplinas de la inteligencia para la recolección de información OSINT, HUMINT, TECHINT y GEOINT.

Fuentes abiertas (OSINT):

Son fuentes de información públicamente accesibles como blogs de seguridad y redes sociales, usado para investigar indicadores de seguridad que se publican y analizar nuevas campañas de malware, también sirve para identificar dentro de los PIRs estratégicos fuentes de difamación y posibles riesgos externos que pueden afectar nuestra organización. Herramientas OpenSource como **TheHarvester** se utiliza para la recolección pasiva de información como correos electrónicos y subdominios de fuentes publica, **SpiderFoot** automatiza la recopilación de Inteligencia sobre un objetivo consultando ciento de fuentes de datos, otras técnicas utilizadas son script personalizados para la automatización de la extracción de información de blogs, redes sociales y foros por medio de Scrapers y Crawlers.

Los repositorios de código como Github ofrecen una fuente de datos tanto de código malicioso como de listas de IoCs.

Fuentes Humanas (HUMINT):

Esta categoría incluye información que es obtenida a través de la interacción humana y la colaboración lo que proporciona un contexto que los datos por sí solo no pueden ofrecer.

Este se asocia a la información que los empleados reportan como intentos de phishing que filtros de seguridad previos no pudo filtrar, intentos de ingeniería social que estén dirigidos bajo un contexto especifico o general. La importancia de establecer canales de comunicación abiertos para el reporte de incidencias es fundamental para la obtención de información de la operación de los empleados, se pueden usar plataformas como **GLPI** para el reporte de los usuarios dentro de la organización para que luego esta información pueda ser llevada y analizada por el centro de seguridad.

Otras fuentes de intercambio de la comunidad son grupos de confianza que comparten inteligencia sobre amenazas asociadas al sector. Como ISACs (Centros de Análisis e Intercambio de Información) que se enfocan según el sector o CERTs (Equipo de Respuesta a Emergencias Cibernéticas) que se enfocan en la prevención y respuesta a incidentes de seguridad digital. Para Colombia es ColCERT.

Fuentes técnicas (TECHINT):

Las fuentes técnicas son los sistemas activos de seguridad que las organizaciones posean como Firewall, Servidores Proxi, Servicios DNS, Antivirus, Honerypot entre otras herramientas de uso común de los usuarios que permita el registro y seguimiento de actividades. Existe una serie de herramientas que permiten concentrar los eventos de estos sistemas para luego ser analizados tales como son los SIEM (Gestión de Información y Eventos de Seguridad) que por medio del protocolo Syslog puede obtener información de diversas fuentes y concentrarla en una sola plataforma. El documento de la NIST la publicación 800-92[33] define y documenta la estandarización para la administración de los eventos de seguridad, este documento deja a disposición una serie de recomendaciones en el tratamiento y procesamiento de los logs como también la estandarización de formatos de los eventos los cuales los más comunes es el formato Syslog que es el estándar para la generación, envió y almacenamiento de mensajes de sistemas de red y servidores, el CEF (Common Event Format) que es el formato de registro estandarizado para la seguridad que se construye sobre syslog, permite a los dispositivos de seguridad y otros sistemas enviar datos y eventos de consola y LEEF (Log Event Extende Format) que es otro formato utilizado para enviar los de seguridad que es similar al CEF pero varia el formato de envió.

En la actualidad otra fuente de información son las API de plataformas que ofrecen servicios como Office365, GCP, Azure, AWS y otros productos hospedados externamente y que manejan los usuarios de la organización donde dan acceso a registros de auditoria en un formato JSON siendo esta otra fuente de información.

Fuente geoespacial (GEOINT):

Si vienen esta fuente esta más orientada a la consulta y al seguimiento de eventos de seguridad con orígenes comunes, este tipo de información ayuda a recolectar métricas sobre los eventos de seguridad y sus orígenes para poder crear reglas más cerradas sobre los orígenes y actores con mayor interés en ataques basado en su ubicación geográfica. Una fuente consulta y más utilizada es MaxMind. La información de MaxMind es utilizada por investigadores para obtener inteligencia sobre la ubicación de una dirección IP, lo cual es útil para la detección de fraude y la seguridad. Está estrechamente relacionada con las OSINT como una fuente de información abierta.

Fase de procesamiento de datos:

En esta fase las herramientas que necesitamos son las que permite recolectar información de diversas fuentes y

normalizarla en un solo formato, estas herramientas son más conocidas como SIEM (Gestión de Información y Eventos de Seguridad) que ayudan a procesar y almacenar los eventos de seguridad.

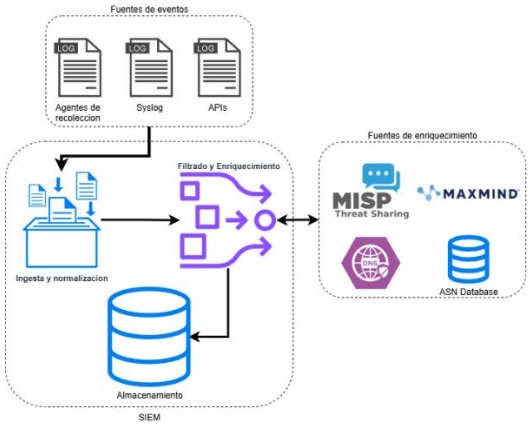


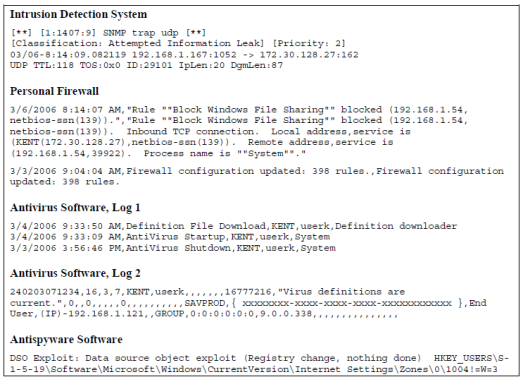
Fig. 3 Función de un SIEM (Propia)

Las fuentes de la Fase de recolección tienen diferentes propósitos y objetivos que en la fase de recolección se comienza a estructurar con el fin también de correlacionar eventos y enriquecer la información obtenida. Esta fase se constituye de 3 pasos clave.

Ingesta y normalización:

Existen tres tipos comunes en los que se puede tener acceso a las diversas fuentes de información, una es la que se establece en una relación de cliente-servidor entre el SIEM y los equipos que manejan servicios de log locales tales como los sistemas operativos Windows y Linux (Sus diversas versiones) que en su gran medida son servidores que hospedan otras aplicaciones o en los que se hacen diversas operaciones. Esta relación le permite enrutar los eventos del sistema o los registros de auditoría. Otro es por medio del reenvío de los logs a otro servidor de Syslog esta operación es común en sistemas embebidos en los que no se pueden realizar instalaciones como firewall, switch o sistemas cerrados que impiden operaciones locales complejas más allá del propósito de su instalación, y el ultimo es por medio de consultas remotas a APIs de proveedores se servicios en las diferentes escalas como IaaS, PaaS o SaaS que al no tener acceso local a los servicios la integración directa de auditoria se publica en un endpoint que debe ser consultado de manera remota.

Los eventos recolectados varían según su formato, origen y datos que proporcionan por lo que un proceso importante dentro del proceso es la estandarización de los diferentes formatos a uno común, este formato en gran medida este formato esta dado en JSON y el almacenado como un documento como se mencionó anteriormente. La estructura de este documento está dada por una objetos o etiquetas en los que se organizan y estructuran los logs.



Intrusion Detection System

```
[**] [1:1407:9] SNMP trap udp [**]
[Classification: Attempted Information Leak] [Priority: 2]
03/06-8:14:09.082119 192.168.1.167:1052 -> 172.30.128.27:162
UDP TTL:118 TOS:0x0 ID:29101 IpLen:20 DgmLen:87
```

Personal Firewall

```
3/6/2006 8:14:07 AM,"Rule ""Block Windows File Sharing"" blocked (192.168.1.54,
netbios-ssn(139)).","Rule ""Block Windows File Sharing"" blocked (192.168.1.54,
netbios-ssn(139)).  Inbound TCP connection.  Local address,service is
(KENT(172.30.128.27),netbios-ssn(139)).  Remote address,service is
(192.168.1.54,39922).  Process name is ""System"".""

3/3/2006 9:04:04 AM,Firewall configuration updated: 398 rules.,Firewall configuration
updated: 398 rules.
```

Antivirus Software, Log 1

```
3/4/2006 9:33:50 AM,Definition File Download,KENT,userk,Definition downloader
3/4/2006 9:33:09 AM,AntiVirus Startup,KENT,userk,System
3/3/2006 3:56:46 PM,AntiVirus Shutdown,KENT,userk,System
```

Antivirus Software, Log 2

```
240203071234,16,3,7,KENT,userk,,,,,,,16777216,"Virus definitions are
current.",0,,0,,,,,0,,,,,,,,,SAVPROD,{ xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx },End
User,(IP)-192.168.1.121,,GROUP,0:0:0:0:0:0,9.0.0.338,,,,,,,,,,,,,,
```

Antispyware Software

```
DSO Exploit: Data source object exploit (Registry change, nothing done)  HKEY_USERS\S-
1-5-19\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\0\1004!=W=3
```

Fig. 4 Ejemplos de entradas en el registro del software de seguridad [33]

Los logs llegan con diferentes formatos y datos por ello los sistemas de SIEM tienen unos decodificadores que en muchos casos se basan en producto o tecnología que permite extraer valores de una cadena de datos por medio de expresiones regulares y el análisis de indicadores comunes entre los diferentes logs, lo que hace que según el origen del log o su estructura se ejecute el decodificador respectivo para extraer los datos del log en formato RAW pasarlo a un formato más fácil de manipular como JSON asignándole una clave valor según los datos extraídos.

Esta primera clave es una de las más importantes en la de procesamiento de información ya que se pueden quitar datos del log que no aporta información relevante y solo extraer la información necesaria.

Filtrado y enriquecimiento:

Con los eventos o logs estructurados en un formato común se pueden aplicar reglas de procesamiento que permiten a partir de las etiquetas realizar búsquedas profundas de los Indicadores de compromiso que detectemos y buscar en otras fuentes de datos para ampliar la información relacionada con el evento.

Los logs son filtrados a partir de reglas que le da un criterio validando el tipo de evento y clasificándolo según gravedad e impacto. Existen tres tipos de eventos comunes los cuales el primero son los eventos que constituyen a los registros informativos sobre operaciones que no precisamente implica un evento de seguridad sino que solo detalla acciones por el usuario que su objetivo es informar una operación o acción, están los eventos que se desencadenan aparir de un incidente que se atribuye a una acción que en un principio va contra las configuraciones de seguridad, es decir, eventos que están relacionadas a intenciones maliciosas tales como inicios de sesión fallidos o ataques que influyan estos eventos se pueden relacionar a los registrados en el marco de trabajo como MITRE ATT&CK [22]. El ultimo tipo de evento son los relacionados a violaciones de seguridad que son incidentes confirmadas donde ya existe un acceso no autorizado o una operación exitosa de intrusión.

A partir del tipo los SIEM aplican las reglas y los asocian a diferentes estándares de la industria para darles un peso y valor a la información recolectada y de esta manera priorizar y filtrar los eventos que son más importantes donde según el estándar y la política interna un evento puede tener un peso mayor o menor, pero en la estandarización se le atribuye un valor de seguridad diferente y una aplicabilidad según la organización. Los estándares de seguridad más comunes son PCI DSS (Payment Card Industry Data Security Standard), GDPR (General Data Protection Regulation), HIPAA (Health Insurance Portability and Accountability Act), NIST 800-53 (National Institute of Standards and Technology - Security and Privacy Controls), TSC (Trust Services Criteria) e ISO27001.

Para la gestión de eventos de seguridad resalta una que es **Wazuh** la cual opera bajo la licencia publica GNU y la licencia Apache 2.0, esta herramienta maneja una alta compatibilidad con la recolección de eventos de diferentes fuentes por medio de decodificadores más comunes de la industria que permiten extraer información de eventos se seguridad de manera nativa, al ser de código libre permite crear decodificadores propios para extraer información de eventos específicos aceptando múltiples fuentes, adicional ofreciendo acciones extendidas que le da un valor agregado a la herramienta. También cuenta con una integración nativa de reglas asociadas a los estándares por lo que facilita su adopción y aplicación a las industrias que requieran aplicar controles de seguridad basado en estándares.

Para ampliar la información de los eventos usamos conectores que enriquezcan la información obtenida por ejemplo son las direcciones IP en una transacción de un log de un Firewall, el equipo firewall da IoC que es la IP del evento pero no más información aparte de la acción, una acción común seria el bloqueo de la IP pero esto da información sobre patrones o los orígenes por lo que se puede consultar una fuente externa pública de inteligencia para correlacionar la dirección IP a más eventos u obtener información más detallada como el país, su resolución inversa (rDNS), si esta listada en un RBL y demás información que podamos obtener de estas fuentes públicas. Con esto un indicador común como IP se le puede ampliar la información y construir un evento más completo y enriquecer la información.

Esto aplica a diversos Indicadores de compromiso que podamos usar, las fuentes OSINT son las contienen una mayor cobertura para realizar estas integraciones. **MISP** cuenta con una serie de conectores que permite consultar diferentes fuentes de información para validar todos los IoC y permite su integración libre con los SIEM.

Existe una plataforma utilizada para la inteligencia de amenazas que es **OpenCTI** que opera bajo la licencia Apache 2.0 en su versión comunitaria la cual tiene una amplia gama de funciones que permite procesar y correlacionar las alertas generadas por el SIEM y a partir de búsquedas en fuentes abiertas relacionar los eventos a diferentes actores comunes en el mundo permitiendo una gestión centralizada de la inteligencia y permitiendo una integración general dentro del ciclo de vida de inteligencia. Utiliza estándares de la industria como STIX2 [5].

La integración de un SIEM como **Wazuh**, un OSINT como **MISP** y CTI como **OpenCTI** para el núcleo del ciclo de vida de inteligencia aporta un valor importante en la reducción de costos de licenciamiento y una mejora significativa de seguridad para las organizaciones que requieran mejorar la observabilidad de seguridad.

Almacenamiento:

Los datos se almacenan en bases de datos optimizadas en la búsqueda y correlación como **OpenSearch** que es una suite de búsqueda y análisis distribuida de código abierto que trabaja con licencia de Apache 2.0, la herramienta de Wazuh almacena los eventos de seguridad sobre esta tecnología lo que le permite manejar un gran flujo de datos sin tener restricciones de procesamiento o capacidad almacenamiento por lo que el límite de almacenamiento está definido es por la capacidad de la infraestructura.

Fase de análisis de información:

En esta fase esta más orientada a la participación humana donde los equipos de tecnología tienen que a partir de los datos obtenidos relacionar los eventos y aplicar una de las técnicas de diagnóstico (KAC, QOI, ACH, etc) [24]para analizar la información. Si vienen las herramientas como Wazuh realiza una asociación a reglas ya establecidas a Tácticas, Técnicas y Procedimientos (TTPs) basado en el marco de trabajo de MITRE ATT&CK no exime de la responsabilidad de analizar los datos y generar una interpretación autónoma de la información recolectada. Esta fase es un recordatorio de no aplicar malas prácticas como “Configurar y olvidar” donde se confía completamente de las herramientas y se olvida del factor humano para la interpretación.

Si bien una herramienta bien configurada reduce y filtra la información que se debe procesar no se puede dejar de analizar y aplicar las acciones que sean requeridas para los eventos generados. Para ello se pueden usar herramientas como **DFIR-IRIS** que trabaja bajo la licencia LGPL-3.0 que permite crear un sistema para la respuesta a incidentes y de esta manera crear casos de seguimiento a incidentes para documentar los casos y de manera activa dar seguimiento a las incidencias donde se puedan tomar acciones reales y documentadas.

Esta herramienta permite integrar soluciones de seguridad como SIEM que generan las alertas automáticas y que cree un caso en la plataforma para darle seguimiento esto cumpliendo con los objetivos de la fase 1 relacionado a los objetivos operaciones para los equipos de respuesta a incidentes.

Es importante generar un informe de la inteligencia adaptado a la audiencia (Estratégica, táctica y operacional). Este producto no es un resumen sino una evaluación del análisis sobre el significado de los hallazgos que busca también generar

una perspectiva a futuro sobre lo que puede ocurrir y cuáles son las acciones que se pueden tomar al respecto [16].

Fase de difusión y retroalimentación:

La manera en que se difunde la información es importante para el ciclo ya que de esta se puede obtener retroalimentación de los resultados y con esto establecer mejoras en el proceso u optar por tomar decisiones más precisas frente a la respuesta de amenazas.

En la difusión se deben entregar los resultados del análisis y ya producida a las partes interesadas de tal manera que según su contexto puedan entender y ser utilizadas para tomar decisiones. La manera en la se que deben tomar decisiones varía según el público objetivo para una audiencia estratégica la información más asertiva para su análisis y toma de decisiones esta mas orientado al impacto y la relación de afectación y riesgo de las amenazas con el fin de que si hay que tomar acciones con una afectación económica o de inversión tener la información necesaria para justificar las acciones a tomar. Para las audiencias mas tácticas comprender las metodologías del ataque y su impacto es mas importante para tomar medidas mas especificas en la técnica para mitigar estas amenazas. La audiencia orientada a la operación es importante tener información mas precisa sobre los indicadores de compromiso y el impacto que este tiene a la operación en especifica como las acciones a tomar en caso de un evento de seguridad.

Existen unos principios claves que son: “la inteligencia correcta”, “a la persona correcta”, “en el formato correcto” y “en el momento oportuno”.

Audiencia y Formato:

Estratégico (C-Suite): Recibe informes ejecutivos breves o presentaciones que se centran en el riesgo para el negocio, el impacto financiero y la toma de decisiones de inversión a largo plazo.

Táctico (Equipos de Seguridad): Recibe informes técnicos sobre las Tácticas, Técnicas y Procedimientos (TTPs) de los adversarios. El objetivo es que puedan ajustar las defensas y arquitecturas de seguridad.

Operacional (SOC): Recibe alertas en tiempo real e Indicadores de Compromiso (IoCs) a través de feeds automatizados o sistemas de tickets para bloquear amenazas inmediatas por medio de sistemas como DFIR-IRIS o integraciones con GLPI y Webhooks actualmente se pueden realizar integraciones con herramientas de mensajería como Microsoft Teams, Telegram, Correo electrónico y WhatsApp.

Oportunidad:

Una inteligencia brillante entregada demasiado tarde es inútil. Las alertas operacionales deben ser instantáneas, mientras que los informes estratégicos pueden ser mensuales o trimestrales [7].

La retroalimentación le da la vuelta a la fase de Dirección y Planificación siendo el componente de control de calidad del todo el ciclo.

El objetivo de la retroalimentación es responder a los PIRs de la fase 1 donde evaluamos si se cumplieron de manera efectiva y objetiva si se cumplieron. Esta retroalimentación se realiza por medio de reuniones regulares de seguimiento del sistema donde se evalúa si los informes fueron de utilidad y darle seguimiento a la implementación de los IoCs que envían desde el SIEM.

La retroalimentación asertiva permite refinar los PIRs con el fin de que si hay que realizar algún ajuste sobre la manera en la se recrea la información o se analiza los eventos de seguridad se puedan tomar las acciones con el fin que con cada iteración se pueda fortalecer el CTI volviéndose cada vez mas inteligente y relevante.

IV. ARQUITECTURA PROPUESTA

De acuerdo con las herramientas mencionadas una arquitectura mas centrada a un CTI a partir de herramientas Open Source puede ser la siguiente, si bien los requisitos de operación de cada herramienta pueden variar y el nivel de integración de cada una puede variar el objetivo es establecer las herramientas que permiten un ecosistema de CTI robusto.

La propuesta busca dar la guía para la toma de decisiones a la hora de construir un CTI con herramientas libres con el fin de dar vista a la facilidad y abrir la posibilidad de aplicar ecosistemas robustos sin depender de una suscripción, se debe tener en cuenta que se debe contar con una arquitectura de Hardware capaz de soportar las herramientas.

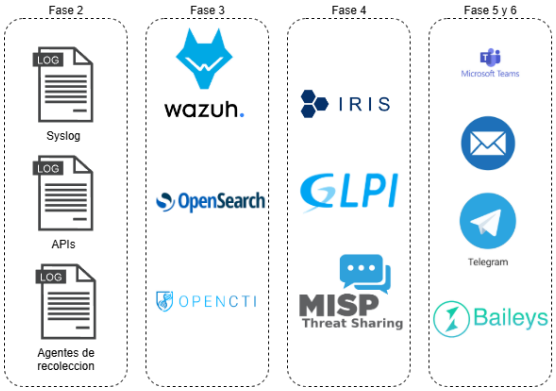


Fig. 4 Arquitectura de Herramientas (Propia)

A continuación, se relacionan las herramientas y su respectiva fuente para su documentación también su método de despliegue se encuentra en la documentación y su soporte es amplio en la comunidad de cada proyecto, un proyecto para desarrollos propies puede ser Baileys el cual ofrece una integración con Whatsapp Web para crear aplicaciones de integración para enviar alertas vía Whatsapp.

TABLA II
PROYECTOS ECOSISTEMA CTI [6]

PROYECTO	URL
Wazuh (GPLv2-ALv2)	https://wazuh.com/
OpenSearch (ALv2)	https://opensearch.org/
OpenCTI (ALv2)	https://filigran.io/platforms/opencti/
DFIR-IRIS (LGPLv3)	https://www.dfir-iris.org/
GLPI (GPLv3)	https://www.glpi-project.org/en/
MISP (AGPL-3.0)	https://www.misp-project.org/
Baileys (MIT)	https://baileys.wiki/docs/intro/

Estos proyectos de manera individual son de alto valor para el ecosistema y pueden ser instalados de manera individual o escoger los que se adapten mejor a nuestro PIRs y generar integraciones entre ellos o herramientas ya existentes dentro de las organizaciones.

V. RESULTADOS

Realizando un estudio sobre la posible adopción de proyectos OpenSource se realizó una en cuesta de 10 preguntas con el fin de determinar la viabilidad y las limitaciones que se ven en las organizaciones a la hora de optar por la implementación de un CTI con herramientas de código libre, de las cuales se analizaron y trabajaron durante el ejercicio en los resultados de viabilidad tomamos 3 preguntas para su evaluación. Las demás pueden ser consultadas dentro de un anexo.

Las dos principales limitaciones de las organizaciones para adoptar mecanismos de seguridad son los altos costos con un 44% y la falta de conocimiento sobre el tema de seguridad con un 31%, esto hace ver que el uso de herramientas de código abierto elimina esta barrera ya que al es libre y con documentación publica y de la comunidad es una opción sustentable a la hora de implementar dentro de una organización.



Fig. 5 Pregunta encuesta Numero 1 (Propia)

También se observa una alta tendencia de los usuarios sobre los IoCs que son más básicos y que por si solos no aportan un valor informativo significativo para su análisis donde las Direcciones IP de los atacantes sin información útil adicional no aporta un valor relevante para el 56% de los encuestados y los dominios asociados a malware con el 19%, por esto es importante la integración con fuentes de inteligencia que enriquezcan las métricas más básicas y aportar valor a la información.



Fig. 6 Pregunta encuesta Numero 4 (Propia)

Una fase fundamental del ciclo de vida es el análisis de los datos la mayoría de los usuarios tiene una tendencia positiva sobre el seguimiento y análisis de registro de seguridad donde la mayoría los revisa como mínimo cada 15 días con un 38% y cada 7 días con un 31% lo que representa un interés inicial sobre conocer el estado de seguridad de la organización esto hace que sea más fácil la adopción de sistemas como SIEM para automatizar la ingesta y seguimiento de eventos de seguridad lo permitiría la optimización en la respuesta a posibles eventos que no vemos en los intervalos en los que no accedemos a estos registros.



Fig. 7 Pregunta encuesta Numero 10 (Propia)

VI.CONCLUSIONES

Durante el ejercicio de investigación se vislumbró que existe un proceso lógico y organizado para la gestión de seguridad de las organizaciones lo que se puede asociar en algunas ocasiones a un proceso que de manera natural que seguimos para la gestión de seguridad. Estructurar y organizar los sistemas de seguridad permite optimizar la gestión de recursos y optimizar los tiempos de respuesta a incidentes.

También se pudo observar que aplicar sistemas de seguridad con una estructura compleja y organizada no requiere de herramientas pagas sino que como línea de partida se puede iniciar con herramientas de código abierto para gestionar un ecosistema de seguridad robusto y escalable lo que permite cerrar la brecha de seguridad de muchas organizaciones que tienen limitaciones tanto económicas como también del talento humano que se requiere ya que esto permite acceder a la documentación y conocimiento de muchas fuentes de inteligencia que su objetivo es fortalecer la resiliencia a los incidentes de seguridad.

El alto crecimiento de vectores de amenazas que se generan a partir de las nuevas tecnologías que surgen todos los días; es importante optar por mecanismos y metodologías que permitan adaptar y crecer junto a estos riesgos para que no exista una brecha de seguridad importante dentro de nuestro entorno corporativo también buscar eliminar esa resistencia a la aplicación de mecanismos de seguridad bajo la premisa de que nuestras organizaciones no son un objetivo, en la actualidad cualquier organización o usuario legitimo conectado a la red es una potencial victima por lo que el riesgo es general y no discrimina por tipo de organización.

VII. REFERENCIAS

[1] D. D. Suárez Medina, "Entrevista a Jeimy José Cano Martínez. La preparación para enfrentar ciberamenazas sofisticadas," Ciberespacio, Tecnología e Innovación, vol. 3, no. 5, pp. 107-112, 2024. DOI: 10.25062/2955-0270.4871.

[2] R. M. Lee, "The Sliding Scale of Cyber Security," SANS Institute, Reading, MA, USA, White Paper, Nov. 2015. [Online]. Disponible en: https://www.sans.org/white-papers/36240/

[3] Awan, M., Alam, A., & Kamran, M. (2025). Cybersecurity Challenges in Small and Medium Enterprises: A Scoping Review. Journal of Cyber Security and Risk Auditing, 2025(3), 89–102. https://doi.org/10.63180/jcsra.thestap.2025.3.7

[4] A. Dulaunoy, A. Iklody, and G. Wagener, "MISP: The Design and Implementation of a Collaborative Threat Intelligence Sharing Platform," in Proc. 2016 ACM Workshop Inf. Sharing Collab. Security, Vienna, Austria, 2016, pp. 49–56. DOI: 10.1145/2994539.2994542.

[5] S. Barnum, "Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX™)," The MITRE Corporation, Bedford, MA, USA, White Paper, Apr. 2012.

[6] Gartner, "Threat Intelligence (TI)," Gartner Glossary. [En línea]. Disponible en: https://www.gartner.com/en/information-technology/glossary/threat-intelligence-ti

[7] Shackleford, D. (2015). "Who's Using Cyberthreat Intelligence and How?". SANS Institute Reading Room. Disponible en: https://cdn-cybersecurity.att.com/docs/SANS-Cyber-Threat-Intelligence-Survey-2015.pdf

[8] Caltagirone, S., Pendergast, A., & Betz, C. (2013). "The Diamond Model of Intrusion Analysis". Applied Network Solutions. Disponible en: https://apps.dtic.mil/sti/citations/ADA586960

[9] The MITRE Corporation, "MITRE ATT&CK®," MITRE ATT&CK®, 2024. [En linea]. Disponible en: https://attack.mitre.org/

[10] CrowdStrike, "What is an Indicator of Compromise (IoC)?" CrowdStrike, 2 de agosto de 2024. [En línea]. Disponible en: https://www.crowdstrike.com/cybersecurity-101/indicators-of-compromise/

[11] N. Chism, "Threat Intelligence: An Introduction for Beginners," SANS Institute, Reading, MA, USA, White Paper, 2016.

[12] R. M. Lee, "Cyber Threat Intelligence," Hoboken, NJ, USA: John Wiley & Sons, 2023.

[13] B. Cinar, "Cyber Threat Intelligence: Current Trends and Future Perspectives," J. Eng. Res. Rep., vol. 25, no. 4, pp. 91–105, 2023. DOI: 10.9734/JERR/2023/v25i4905.

[14] C. M. Salamanca, G. A. Aguilar Restrepo, y J. D. Cornejo Pinzón, "El papel de la CIA (Ciberinteligencia de Amenazas) dentro de las ciberamenazas que afectan las PYMES," Proyecto de Grado, Fac. de Ing. y Ciencias Básicas, Fundación Universitaria Los Libertadores, Bogotá, Colombia, 2021. [En línea]. Disponible en: http://hdl.handle.net/11371/6657

[15] A. Gioti, "Advancements in Open Source Intelligence (OSINT) Techniques and the role of Artificial Intelligence in Cyber Threat Intelligence (CTI)," disertación, Dept. Sistemas Digitales, Univ. Piraeus, Piraeus, Grecia, 2024, p. 11, DOI: http://dx.doi.org/10.26267/unipi_dione/3728.

[16] M. Phythian, (Ed.), Understanding the Intelligence Cycle. London, UK: Routledge, 2013. DOI: 10.4324/9780203558478.

[17] Micro Focus, "Implementing ArcSight Common Event Format (CEF)," Documentación Técnica de ArcSight, 2023. [En línea]. Disponible en: https://www.microfocus.com/documentation/arcsight/arcsight-smartconnectors-8.4/pdfdoc/cef-implementation-standard/cef-implementation-standard.pdf

[18] N. Prasad, A. Diro, M. Warren, y M. Fernando, "A survey of cyber threat attribution: Challenges, techniques, and future directions," Computers & Security, vol. 157, Art. no. 104606, 2025. DOI: 10.1016/j.cose.2025.104606.

[19] W. Tounsi and H. Rais, "A survey on technical threat intelligence in the age of sophisticated cyber attacks," Computers & Security, vol. 72, pp. 212-233, Jan. 2018. DOI: 10.1016/j.cose.2017.09.001

[20] B. Jordan, R. Piazza, y T. Darley, (Eds.), "STIX Version 2.1," OASIS Standard, 10 de junio de 2021. [En línea]. Disponible en: https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html

[21] B. Jordan y D. Varner, (Eds.), "TAXII Version 2.1," OASIS Standard, jun. 2021. [En línea]. Disponible en: https://docs.oasis-open.org/cti/taxii/v2.1/os/taxii-v2.1-os.html

[22] The MITRE Corporation, "MITRE ATT&CK® Enterprise tactics," MITRE ATT&CK®, 2024. [En linea]. Disponible en: https://attack.mitre.org/tactics/enterprise/

[23] The MITRE Corporation, "MITRE ATT&CK® Enterprise Techniques," MITRE ATT&CK®, 2024. [En linea]. Disponible en: https://attack.mitre.org/techniques/enterprise/

[24] R. J. Heuer, Jr., Psychology of Intelligence Analysis. Langley, VA, USA: Center for the Study of Intelligence, Central Intelligence Agency, 1999. [En línea]. Disponible en: https://www.cia.gov/resources/csi/books-monographs/psychology-of-intelligence-analysis-2/

[25] Central Intelligence Agency, A Tradecraft Primer: Structured Analysis in the DI, Langley, VA, USA: Center for the Study of Intelligence, 2005. [En línea]. Disponible en: https://www.cia.gov/resources/csi/static/Tradecraft-Primer-apr09.pdf

[26] IRIS-Project, "DFIR-IRIS," DFIR-IRIS, 2025. [En línea]. Disponible en: https://www.dfir-iris.com/

[27] S. Phipps, "Open source needs to clean up its language," InfoWorld, 1 de noviembre de 2013. [En línea]. Disponible en: https://www.infoworld.com/article/2205095/open-source-needs-to-clean-up-its-language.html

[28] Apache Software Foundation, "Apache License, Version 2.0," ene. 2004. [En línea]. Disponible en: https://www.apache.org/licenses/LICENSE-2.0

[29] Free Software Foundation, "What is Copyleft?," [En línea]. Disponible en: https://www.gnu.org/licenses/copyleft.html

[30] Free Software Foundation Europe (FSFE), Software Libre. Disponible en: https://fsfe.org/freesoftware/freesoftware.es.html.

[31] Proyecto GNU, ¿Qué es el Software Libre? Disponible en: https://www.gnu.org/philosophy/free-sw.es.html.

[32] G. S. Rodríguez, "El software libre y sus implicaciones jurídicas," Revista de Derecho, no. 30, pp. 206-231, dic. 2008. [En línea]. Disponible en: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0121-86972008000200009

[33] K. Kent y M. Souppaya, "Guide to Computer Security Log Management," National Institute of Standards and Technology, Gaithersburg, MD, USA, NIST Special Publication 800-92, sep. 2006. [En línea]. Disponible en: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-92.pdf