



**GUÍA DE SEGURIDAD
(CCN-STIC-425)**

**CICLO DE INTELIGENCIA Y ANÁLISIS DE
INTRUSIONES**

OCTUBRE, 2015

Edita:



© Editor y Centro Criptológico Nacional, 2015

NIPO: 002-15-028-6

Fecha de Edición octubre de 2015

El Sr. Carlos Galán ha participado en la elaboración del presente documento.

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del **Centro Criptológico Nacional**, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

PRÓLOGO

Entre los elementos más característicos del actual escenario nacional e internacional figura el desarrollo alcanzado por las Tecnologías de la Información y las Comunicaciones (TIC), así como los riesgos emergentes asociados a su utilización. La Administración no es ajena a este escenario, y el desarrollo, adquisición, conservación y utilización segura de las TIC por parte de la Administración es necesario para garantizar su funcionamiento eficaz al servicio del ciudadano y de los intereses nacionales.

Partiendo del conocimiento y la experiencia del Centro sobre amenazas y vulnerabilidades en materia de riesgos emergentes, la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional en su artículo 9.2.f).

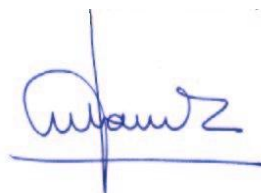
Una de las funciones más destacables que, asigna al mismo, el Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional es la de elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración.

La ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, en su artículo 42.2 crea del Esquema Nacional de Seguridad (ENS), que establece las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos.

El Real Decreto 3/2010 de 8 de Enero desarrolla el Esquema Nacional de Seguridad y fija los principios básicos y requisitos mínimos así como las medidas de protección a implantar en los sistemas de la Administración. En su artículo 29 se autoriza que a través de la series CCN-STIC el CCN desarrolle lo establecido en el mismo.

La serie de documentos CCN-STIC se ha elaborado para dar cumplimiento a esta función y a lo reflejado en el ENS, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Octubre, 2015



Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

1.	OBJETO DE ESTE DOCUMENTO.....	5
2.	LA INTELIGENCIA EN MATERIA DE CIBERSEGURIDAD	5
2.1.	DEFINICIÓN Y UTILIZACIÓN DE LA INTELIGENCIA.....	5
2.2.	EL CICLO DE INTELIGENCIA	6
2.2.1	DIRECCIÓN Y PLANIFICACIÓN.....	7
2.2.2	RECOLECCIÓN	7
2.2.3	TRANSFORMACIÓN	9
2.2.4	ANÁLISIS Y PRODUCCIÓN	10
2.2.5	DIFUSIÓN.....	11
2.2.6	EVALUACIÓN	13
3.	UN MODELO PARA EL ANÁLISIS DE INTRUSIONES: EL MODELO DE DIAMANTE	13
3.1.	INTRODUCCIÓN AL MODELO.....	14
3.2.	EL EVENTO.....	16
3.2.1	EL ADVERSARIO	17
3.2.2	LA CAPACIDAD	18
3.2.3	LA INFRAESTRUCTURA	18
3.2.4	LA VÍCTIMA.....	19
3.2.5	LAS META-CARACTERÍSTICAS	20
3.3.	EXTENSIÓN DEL MODELO.....	22
3.4.	INDICADORES DE CONTEXTO	25
3.5.	ANÁLISIS DIRIGIDO	25
3.5.1	ORIGEN DEL ANÁLISIS	26
3.6.	LOS HILOS DE ACTIVIDAD	28
3.6.1	EL PROCESO DEL ADVERSARIO	31
3.6.2	SOPORTE AL ANÁLISIS DE HIPÓTESIS	32
3.7.	GRUPOS DE ACTIVIDAD	34
3.7.1	PASO 1: EL PROBLEMA A ANALIZAR.....	36
3.7.2	PASO 2: SELECCIÓN DE CARACTERÍSTICAS.....	36
3.7.3	PASO 3: CREACIÓN	38
3.7.4	PASO 4: CRECIMIENTO.....	40
3.7.5	PASO 5: ANÁLISIS.....	40
3.7.6	PASO 6: REDEFINICIÓN.....	41
3.7.7	FAMILIAS DE GRUPOS DE ACTIVIDAD.....	41
3.8.	PLANIFICACIÓN.....	42

3.9. CONCLUSIONES DEL MODELO.....	45
ANEXO 1. REFERENCIAS.....	46

1. OBJETO DE ESTE DOCUMENTO

1. Constituye un lugar común afirmar que el uso de las TIC representa uno de los elementos más característicos del actual marco social, político y económico internacional. No obstante, como así señala la Estrategia de Ciberseguridad Nacional, la generalización universal de su uso y la accesibilidad global a las diversas herramientas y redes, facilitando un desarrollo sin precedentes en el intercambio de información y comunicaciones, conlleva, al mismo tiempo, serios riesgos y amenazas que pueden afectar a la Seguridad Nacional.
2. Una de las funciones que la Ley 11/2002, de 6 de mayo, confiere al Centro Nacional de Inteligencia (CNI) es **obtener, evaluar e interpretar información y difundir la inteligencia necesaria para proteger y promover los intereses políticos, económicos, industriales, comerciales y estratégicos de España**, pudiendo actuar dentro o fuera del territorio nacional. Esta misma norma encomienda al CNI, a través del Centro Criptológico Nacional (CCN) el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información y de protección de la información clasificada, a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el CCN, entidad adscrita al CNI y con la que comparte medios, procedimientos, normativa y recursos.
3. Así pues, en base a lo anterior y a lo dispuesto en el Real Decreto 421/2004, de 12 de marzo, por el que se regula el CCN, el presente documento tiene por objeto ofrecer una explicación, simple y concisa, de lo que en ciberseguridad constituye la llamada **Ciberinteligencia** y el **Ciclo de Inteligencia** (epígrafe 2), desarrollando una de sus fases más significativas: el Análisis. Con este propósito se desarrolla un **Modelo para el Análisis Formal de Intrusiones** (epígrafe 3).
4. Con esta publicación, el CCN espera que las Administraciones Públicas españolas, así como las empresas de nuestro país —especialmente aquellas que gestionan intereses estratégicos— y también sus profesionales y ciudadanos se encuentren en mejores condiciones para hacer frente a los riesgos que comporta operar en el ciberespacio.

2. LA INTELIGENCIA EN MATERIA DE CIBERSEGURIDAD

2.1. DEFINICIÓN Y UTILIZACIÓN DE LA INTELIGENCIA

5. A los efectos de esta Guía, definiremos **Inteligencia** como: *“El producto resultante de la recolección, evaluación, análisis, integración e interpretación de toda la información disponible, y que es inmediatamente o potencialmente significativa para la planificación y las operaciones.”*¹
6. Por su parte, definiremos **Ciberinteligencia** como aquellas *“Actividades de inteligencia en soporte de la ciberseguridad. Se trazan ciberamenazas, se analizan las intenciones y oportunidades de los ciberadversarios con el fin de identificar, localizar y atribuir fuentes de ciberataques.”*²
7. Entre las actividades que, en materia del Ciberinteligencia, desarrolla el CNI/CCN se encuentran:

¹ Guía CCN-STIC 401 Glosario y Abreviaturas.

² *Op. Cit.*

- La recopilación de información para que el Gobierno de España, los responsables de las entidades de sus Administraciones Públicas y todos aquellos que constituyen su Comunidad de Inteligencia, puedan conocer la situación real a la que se enfrentan y, en su consecuencia, servir como ayuda para adoptar las decisiones más adecuadas.
 - La producción y difusión de inteligencia.
 - La recolección de información de inteligencia sobre actividades dirigidas contra España o sus intereses, y de la que puedan ser autores estados extranjeros, grupos terroristas y, en general, cualquier agente de la amenaza, directamente o a través de terceros.
 - La dirección y coordinación de acciones dirigidas a proteger los intereses nacionales descritos frente a las antedichas amenazas.
 - El desarrollo de actividades administrativas y de apoyo, tanto dentro de nuestro territorio como fuera de él, que puedan resultar necesarias para el acometimiento de otras actividades de inteligencia.
 - En general, cualesquiera otras actividades que le sean encomendadas por el Presidente del Gobierno, directamente o a través de la Directiva de inteligencia propuesta por la Comisión Delegada del Gobierno para asuntos de Inteligencia.
8. Como quiera que no todas las **organizaciones consumidoras de inteligencia** tienen las mismas necesidades, es por lo que, como luego se verá, lo primero que ha de definir una organización es el tipo de inteligencia que necesita obtener para el más adecuado desempeño de sus funciones o competencias.

2.2. EL CICLO DE INTELIGENCIA

9. Las actividades de inteligencia pueden agruparse en las siguientes seis **fases**:
- Dirección y Planificación.
 - Recolección.
 - Transformación.
 - Análisis y Producción.
 - Difusión.
 - Evaluación.
10. Estas fases se desarrollan cíclicamente, como muestra la figura siguiente.

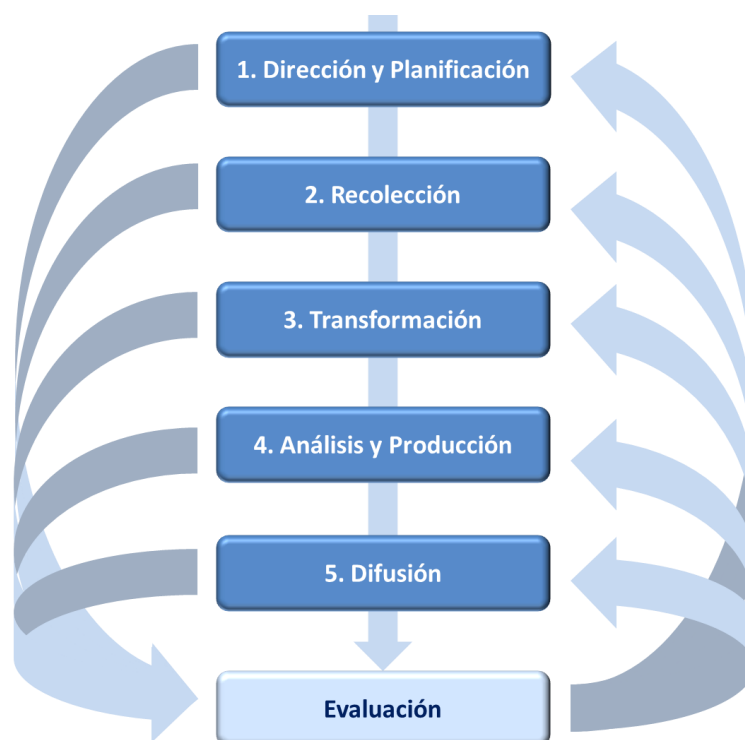


Figura 1. El Ciclo de Inteligencia

11. Así pues, el **Ciclo de Inteligencia** está compuesto por todas aquellas actividades que, de forma ordenada, persiguen la **transformación de información en bruto en inteligencia**, capaz de ser usada por los responsables políticos, administrativos o gerenciales de la organización de que se trate. Este proceso, de naturaleza cíclica, es dinámico y permanente. La última fase de Evaluación tiene lugar tras la ejecución de cada una de las cinco fases restantes, y su objetivo es alinear en cada momento del ciclo los resultados obtenidos de la ejecución de cada fase con sus objetivos.

12. Seguidamente, se incluye una explicación de la función de cada fase.

2.2.1 DIRECCIÓN Y PLANIFICACIÓN

13. El objetivo de esta fase es establecer los **requisitos de inteligencia** de la organización consumidora, así como la **planificación de acciones** tendentes a su obtención.

14. En la fase de Planificación y Dirección se prepara el escenario para el desarrollo del Ciclo de Inteligencia, constituyendo su imprescindible punto de arranque.

15. En la sub-fase de **Dirección (QUÉ)**, las organizaciones consumidoras de inteligencia determinan cuáles han de ser los requisitos del producto que se persigue: por ejemplo, un informe exhaustivo final sobre una determinada materia o asunto. Por su parte, durante la sub-fase de **Planificación (CÓMO)**, la organización consumidora –pudiendo contar con la ayuda de terceros– determina cuáles son las acciones que habrá que desarrollar en las restantes fases del Ciclo de Inteligencia para alcanzar los objetivos perseguidos.

2.2.2 RECOLECCIÓN

16. El objetivo de esta fase es **recopilar los datos en bruto** necesarios (información) para producir el producto final deseado (inteligencia).

17. La recolección de la información en bruto puede tener lugar a través de cinco fuentes básicas:

- Inteligencia Geoespacial, *Geospatial Intelligence* [GEOINT],
- Inteligencia Humana, *Human Intelligence* [HUMINT],
- Inteligencia de Fuentes Abiertas, *Open-Source Intelligence* [OSINT], y
- Inteligencia de Señales, *Signals Intelligence* [SIGINT].

18. Seguidamente, se examinan brevemente tales fuentes.

19. **Inteligencia Geoespacial – GEOINT (*Geospatial Intelligence*)**

La Inteligencia Geoespacial (GEOINT) consiste en la explotación y análisis de imágenes o información geoespacial, para describir, evaluar y representar visualmente las características físicas de los objetos de estudio o de actividades que puedan desarrollarse en la tierra.

20. **Inteligencia Humana – HUMINT (*Human Intelligence*)**

La Inteligencia Humana (HUMINT) se genera a través de la recopilación de información – por vía oral o documental- directamente proveniente de una fuente humana.

Se trata del único tipo de inteligencia en la que los encargados de recabar la información (denominados *oficiales de obtención*) la obtienen directamente de las fuentes (con su conocimiento o no), pudiendo incluso controlar el tema tratado y dirigir la respuesta de la fuente. En muchas ocasiones las fuentes humanas constituyen el único medio de obtener acceso a determinada información.

Existen distintos tipos de HUMINT, desde la denominada **Inteligencia de Alto Nivel**, que comprende información relativa a la Seguridad Nacional o estratégica; hasta la denominada **Inteligencia Específica**, que comprende información de naturaleza táctica.

Como se ha mencionado, HUMINT puede ser adquirida de manera abierta o confidencial.

En la **recolección abierta**, el recolector se reúne con las fuentes, evidenciando abiertamente su condición de representante oficial. La recolección abierta comprende muchas formas de recopilación de información, incluyendo la declaración de personas, informes de origen diplomático, informes policiales, etc.

A diferencia de la anterior, en la **recolección confidencial**, el recolector debe localizar a una persona con acceso a la información deseada, iniciar discretamente una relación con esa fuente para, finalmente, convencer a la fuente a revelar la información que posee. La fuente podrá o no ser informada del carácter oficial de la acción y su interlocutor. Obvio resulta mencionar que el “reclutamiento” de una fuente confidencial puede demorarse meses o, incluso, años, por lo que el mantenimiento de la confidencialidad de la fuente resulta imprescindible.

21. **Inteligencia de Fuentes Abiertas – OSINT (*Open Source Intelligence*)**

La Inteligencia de Fuentes Abiertas (OSINT) es aquella que se produce a través de información públicamente accesible. OSINT se fundamenta en la utilización de una amplia variedad de información y fuentes, entre ellas:

- Medios de comunicación: prensa, radio, televisión, internet...

- Datos públicos: Información derivada de informes gubernamentales o de las Administraciones Públicas, datos oficiales (presupuestos, demografía, debates parlamentarios, ruedas de prensa, conferencias y alocuciones, esquemas y organigramas públicos, declaraciones de impacto medioambiental, etc.)
- Literatura *Gris*: material de acceso controlado, dirigido a comunidades o foros específicos (informes de investigaciones, informes técnicos o económicos, informes de viaje, documentos de trabajo, documentos oficiales, procedimientos, *preprints*, estudios, disertaciones y tesis, documentos comerciales, estudios de mercado, encuestas, boletines, etc.). Generalmente, el material que comprende la Literatura *Gris* se centra en disciplinas científicas, políticas, socioeconómicas y militares.
- Observación e Informes: se trata de información imposible de obtener de otro modo, tal como, imágenes tomadas desde drones, aviones o satélites (v.g. Google Earth), instrumentos que han venido a incrementar la posibilidad de adquirir y procesar información pública que, con anterioridad, sólo podía ser conocida por los Servicios de Inteligencia.

22. Inteligencia de Señales – SIGINT (*Signals Intelligence*)

La Inteligencia de Señales (SIGINT) es aquella que se recaba de las transmisiones de datos, incluyendo la llamada Inteligencia de Comunicaciones (COMINT – *Communications Intelligence*), Inteligencia Electrónica (ELINT – *Electronic Intelligence*) y la Inteligencia de Señales de Instrumentos Extranjeros (FISINT – *Foreign Instrumentation Signals Intelligence*)³.

La producción de inteligencia SIGINT comprende tanto los datos en bruto como su análisis.

2.2.3 TRANSFORMACIÓN

23. Esta fase tiene por objeto convertir el formato de los datos en bruto recabados de las distintas fuentes, en aquellos otros formatos que posibiliten su posterior tratamiento y análisis.
24. La etapa de Transformación exige no sólo el concurso de profesionales de alta cualificación, sino, además, un equipamiento tecnológico sofisticado, capaz de convertir los datos en información útil y procesable. La traducción de datos o de textos (en lengua extranjera, por ejemplo), el descifrado de información, la conversión de datos telemétricos en mediciones con significado, la preparación de la información para su tratamiento informático, almacenamiento o recuperación; y la conversión de informes HUMINT en contenido comprensible son sólo algunos de los procesos de transformación utilizados para la conversión de los datos recabados en información lista para el posterior análisis y producción.

³ COMINT es la inteligencia obtenida mediante el seguimiento de patrones y protocolos (análisis de tráfico), del establecimiento de enlaces entre las partes interconectadas y del análisis del significado de las comunicaciones. FISINT es la información derivada de la interceptación de las emisiones electromagnéticas extranjeras –aéreas, de superficie o subterráneas.

ELINT es la información derivada básicamente de señales electrónicas que no contienen voz o texto (consideradas COMINT). Las fuentes más comunes de ELINT son las señales de radar.

2.2.4 ANÁLISIS Y PRODUCCIÓN

25. El objeto de esta fase es integrar, evaluar, analizar y preparar la información previamente procesada, de cara a obtener el producto final deseado (inteligencia).
26. Al igual que en la anterior, la fase de Análisis y Producción requiere de personal altamente especializado y entrenado (los analistas), capaces de encontrar significado a la información previamente procesada, acompasando y priorizando su análisis en función de los requisitos señalados en la fase inicial de Dirección y Planificación.
27. El resultado de esta fase comprende, esencialmente, lo que se ha dado en llamar ***actionable intelligence***, es decir, un producto de inteligencia capaz de resultar útil y satisfacer las necesidades de su consumidor, de forma directa, sin necesidad de ulterior tratamiento.
28. Como se estudiará en el epígrafe 3 de la presente Guía, el análisis formal y metodológico de los incidentes constituye una pieza esencial de la ciberseguridad, de cara a la provisión de medidas tendentes a mitigar los efectos de tales incidentes.
29. Los analistas de inteligencia -y los ciberanalistas, entre ellos- suelen desarrollar sus funciones sobre un área concreta, que constituye su especialidad, obteniendo la información de todas las fuentes pertinentes, recopilando información, procesándola y realimentando el sistema de análisis con los resultados obtenidos. En Inteligencia y Ciberinteligencia, los resultados del análisis buscan dar respuesta adecuada a una pregunta o cuestión de partida, que el consumidor de inteligencia necesita definir previamente.
30. Así, la actividad de análisis puede esquematizarse del siguiente modo: Los analistas reciben información de entrada, evalúan tal información –poniéndola, incluso, frente a otra información previa o a su propia experiencia personal-, elaboran un “estado de situación” de la actividad bajo análisis y, en último lugar, realizan un pronóstico respecto de lo que es presumible esperar y de la tendencia futura.
31. Por otro lado, como quiera que la obtención de inteligencia responde a un ciclo continuo, el análisis también comprende el desarrollo de los requisitos con los que deberá recopilarse nueva información en el futuro.
32. Finalmente, los resultados obtenidos de una actividad de análisis no deben tomarse como verdades absolutas. En muchas ocasiones, el (ciber)analista –con la ayuda o no de herramientas automatizadas- desarrolla su trabajo con datos, hechos o evidencias incompletas o de confiabilidad relativa. El Modelo de Análisis de Intrusiones que presentamos en el epígrafe 3 de esta Guía tiene en cuenta también la confianza con la que el ciberanalista debe tratar cada característica de un ciberincidente conocido.
33. **Productos obtenidos del análisis:**
 - Inteligencia Actual: La denominada Inteligencia Actual (*Current Intelligence*) aborda los acontecimientos del día a día, tomando en consideración los nuevos descubrimientos o evidencias que se han recabado de un evento concreto, evaluando su importancia, advirtiendo de sus posibles consecuencias a corto plazo y señalando situaciones potencialmente peligrosas para un futuro cercano.
 - Análisis de Tendencias: El Análisis de Tendencias (*Trend Analysis*) –también conocido como “*Informes de Segunda Fase*”- puede proporcionar información sobre un evento o una serie de eventos. Un informe de análisis de tendencias de un evento comprende una valoración sobre si la inteligencia de que se dispone relativa a tal evento es más o menos fiable, información sobre eventos similares, e, incluso,

información básica para familiarizar al lector con el tema. Frecuentemente, la inteligencia generada en el análisis de tendencias se compara con la inteligencia obtenida de otras fuentes, refinándose o matizándose a través de la colaboración de expertos dentro de la Comunidad de Inteligencia.

- Evaluación a Largo Plazo: La Evaluación a Largo Plazo (*Long-Term Assessment*) – también conocida como “*Informes de Tercera Fase*”-, trabajando sobre una amplia base de conocimientos, se ocupa de la evolución futura de la casuística analizada, evaluando posibles tendencias y proporcionando un análisis exhaustivo y detallado de un evento en curso, una sucesión de eventos, un sistema concreto, etc.
- Inteligencia Estimativa: La Inteligencia Estimativa (*Estimative Intelligence*) utiliza escenarios y proyecciones de posibles eventos futuros para evaluar la posibilidad de que ocurran acontecimientos que pudieran afectar a la Seguridad o los sistemas del consumidor de inteligencia. Al abordar las implicaciones del análisis sobre una multiplicidad de posibles resultados y escenarios alternativos, la Inteligencia Estimativa ayuda a los responsables a adoptar medidas de naturaleza estratégica en relación con las amenazas a largo plazo.
- Inteligencia de Avisos: La Inteligencia de Avisos (*Warning Intelligence*) advierte a los responsables de que “algo está ocurriendo o puede ocurrir de forma inminente”. Este tipo de inteligencia transmite una situación de urgencia y suele implicar la necesidad de que los responsables respondan de manera rápida. La Inteligencia de Avisos comprende la identificación o la predicción de eventos (ciberincidentes, en nuestro caso) especialmente importantes.
- Inteligencia de Investigación: La Inteligencia de Investigación (*Research Intelligence*) comprende trabajos, estudios e investigaciones tendentes a desarrollar y apoyar los métodos, procedimientos y herramientas de la Inteligencia Actual y la Inteligencia Estimativa.
- Inteligencia Científica y Técnica: La Inteligencia Científica y Técnica (*Scientific and Technical Intelligence*) contempla el estudio de la evolución técnica, características, rendimiento y capacidades de las tecnologías usadas por los (potenciales) adversarios, incluyendo sus sistemas (ciberarmamento, por ejemplo) y subsistemas. Esta categoría de inteligencia comprende un amplio espectro de disciplinas de naturaleza científica, tecnológica, ciber-armamentística, y la utilización de múltiples recursos en operaciones integradas.

2.2.5 DIFUSIÓN

34. El objeto de esta fase es entregar el producto final al consumidor de inteligencia que lo ha solicitado, así como a otros actores, cuando ello sea necesario y jurídicamente admisible.
35. En esta fase, el consumidor de inteligencia recibe el producto final obtenido de la ejecución sucesiva de las fases anteriores, constituyendo generalmente tal entrega una puesta a disposición o transmisión electrónicas de determinados contenidos: websites, correo electrónico, herramientas de colaboración, distribución de copias en soporte electrónico, etc.
36. Al producto final así obtenido se le denomina **inteligencia acabada**.

37. No obstante lo anterior, en muchas ocasiones es necesario proteger los resultados del análisis (o las fuentes de información), limitando su conocimiento a las personas previamente autorizadas. Por este motivo, muchos Informes de Inteligencia constituyen **información clasificada**⁴. Esta información, sujeta a restricciones de difusión, se divide en **Materias Clasificadas** (definidas en la Ley 9/1968, de 5 de abril, modificada por la Ley 48/78, de 7 de octubre, sobre Secretos Oficiales, como los asuntos, actos, documentos, informaciones, datos y objetos cuyo conocimiento por personas no autorizadas pueda dañar o poner en riesgo la seguridad y defensa del Estado, y que se califican en las categorías de SECRETO y RESERVADO, en atención al grado de protección que requieren) y **Materias Objeto de Reserva Interna**⁵ (definidas como los asuntos, actos, documentos, informaciones, datos y objetos cuyo conocimiento por personas no autorizadas pueda afectar a la seguridad del Estado, amenazar sus intereses o dificultar el cumplimiento de su misión. Se clasifican en las categorías de CONFIDENCIAL y DIFUSIÓN LIMITADA, en atención al grado de protección que requieren)⁶.
38. Una vez que el producto final (inteligencia acabada) ha sido convenientemente difundido podrían todavía identificarse brechas de inteligencia que hicieran necesario completar un nuevo Ciclo de Inteligencia. De ahí que la obtención de inteligencia final se corresponda claramente con un modelo de Mejora Continua.
39. Finalmente, es necesario señalar que el Centro Criptológico Nacional ha puesto en explotación la herramienta **REYES (Repositorio común Y EStructurado de amenazas y código dañino)** como mecanismo para automatizar la compartición de información sobre ciberamenazas.
40. La figura siguiente muestra un mapa conceptual del encaje de REYES con el resto de las herramientas del CCN y los modelos de colaboración previstos con otras instituciones.

⁴ Información Clasificada es cualquier información o material respecto de la cual se decida que requiere protección contra su divulgación no autorizada y a la que se ha asignado, con las formalidades y requisitos previstos en la legislación, una clasificación de seguridad.

⁵ Cuyos precedentes pueden encontrarse en la Política de Seguridad de la Información del Ministerio de Defensa, en los Acuerdos para la Protección de la Información Clasificada con otros países y en diversas Políticas de Seguridad de Organizaciones Internacionales.

⁶ Para mayor información puede consultarse el Anexo II de la Guía CCN-STIC 822 Procedimientos de Seguridad en el ENS.

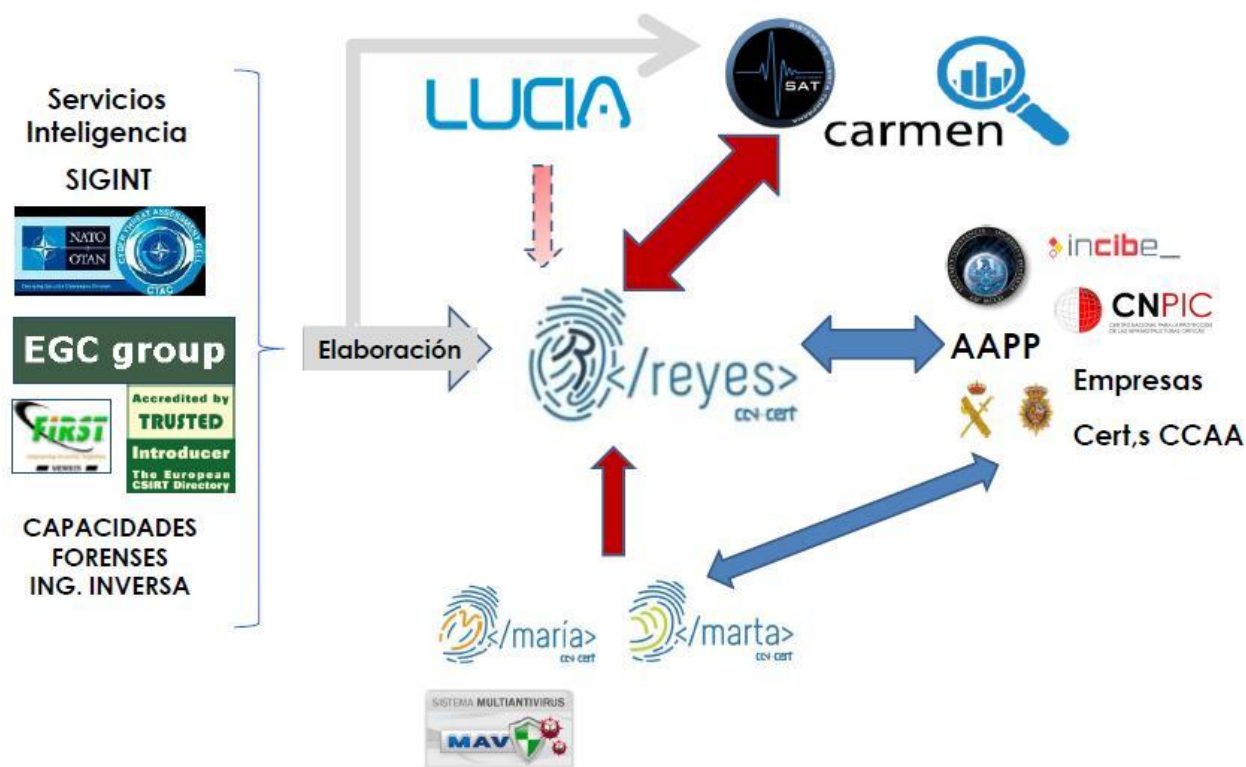


Figura 2: Herramienta REYES

2.2.6 EVALUACIÓN

41. Durante la ejecución de las distintas fases que componen el Ciclo de Inteligencia siempre es posible realimentar cada una de ellas a partir de los resultados obtenidos, utilizando tal realimentación para ajustar y refinar las actividades realizadas, individualmente consideradas, como el Ciclo, en su conjunto.
42. Contar con una evaluación y retroalimentación permanente, por parte no sólo de la dirección de la inteligencia sino también de los que habrán de ser sus consumidores, constituye una medida extraordinariamente importante que permite reajustar en cualquier momento el ciclo de inteligencia, refinando sus actividades y matizando sus análisis, de cara a satisfacer con mayor eficacia las necesidades de inteligencia del consumidor o consumidores finales, en permanente evolución.

3. UN MODELO PARA EL ANÁLISIS DE INTRUSIONES: EL MODELO DE DIAMANTE

43. Dentro de la fase “Análisis y Producción” del Ciclo de Inteligencia, una de las actividades más frecuentes es la denominada **Análisis de Intrusiones**.
44. El Análisis de Intrusiones⁷, que ha venido teniendo lugar desde los primeros ciberataques, pretende, básicamente, dotar a los responsables de seguridad de las organizaciones-víctimas de los métodos, procedimientos y herramientas más adecuados para descubrir, comprender y neutralizar las operaciones del atacante.

⁷ Entenderemos en este epígrafe por “intrusión” cualquier actividad dañina tendente a atacar los sistemas o redes de las víctimas.

45. Como decimos, desde los orígenes de la seguridad de la información el QUIÉN, QUÉ, CUÁNDO, DÓNDE, POR QUÉ y CÓMO, han sido y son las preguntas esenciales a las que el Análisis de Intrusiones, en primera instancia, pretende dar respuesta.
46. Además, el Análisis de Intrusiones tiene como objetivo final proponer medidas de mitigación de impacto, ya sean de naturaleza táctica (contrarrestando la actividad dañina) o estratégica (contrarrestando al adversario⁸).
47. El presente epígrafe desarrolla un modelo de análisis de intrusiones, ampliamente reconocido, el denominado **Modelo del Diamante**⁹, que constituye un método formal que aplica los principios científicos de medida, prueba y repetibilidad al análisis de intrusiones, proporcionando una herramienta simple, formal y completa para la documentación de la actividad de análisis, la síntesis y la correlación de eventos.
48. El modelo expuesto desarrolla la base de una ontología de análisis¹⁰, presentando un marco sobre el que descubrir nuevas actividades dañinas, maximizando las oportunidades de análisis, correlación y síntesis de información nueva, la identificación de los adversarios y mejorando la comunicación y documentación del resultado de los análisis.
49. Formalmente, el modelo constituye un marco matemático que permite la aplicación de la Teoría de Juegos y Grafos y las teorías de clasificación/*clustering*, todo ello de cara a mejorar el proceso de análisis y la toma de decisiones.
50. Como método formal, exhibe varios beneficios:
 - Desarrollo de hipótesis analíticas comprobables, que garanticen la repetibilidad y la exactitud de los resultados,
 - Mayor facilidad para la generación de hipótesis y correlación automatizada a través de eventos,
 - Clasificación rápida y confiable de eventos desarrollados por distintas campañas del adversario,
 - Facilidad para prever los movimientos futuros del adversario, mitigando el impacto de ulteriores acciones dañinas.
51. El modelo, además de general y flexible, posibilita su ampliación con nuevos escenarios, sin dejar de contemplar los conceptos esenciales del análisis de intrusiones¹¹ y las operaciones del adversario.

3.1. INTRODUCCIÓN AL MODELO.

52. El elemento básico del modelo es el denominado *Evento*.

⁸ En este epígrafe utilizaremos, indistintamente, los términos “adversario” o “atacante” para referirnos a los agentes de las amenazas.

⁹ Caltagirone, Pendergast y Betz: The Diamond Model of Intrusion Analysis.

¹⁰ Ver: Leo Obrsta, Penny Chaseb, and Richard Markeloffa. Developing an ontology of the cyber security domain. In Paulo C. G. Costa and Kathryn B. Laskey, editors, Proceedings of Semantic Technologies for Intelligence, Defense, and Security (STIDS) 2012, pages 49–56, October 2012. <http://ceur-ws.org/Vol-966/>

¹¹ Ver: Clifford Stoll. Stalking the wily hacker. Communications of the ACM, 31(5):484–497, May 1988.

Steve Bellovin. There be dragons. In 3rd Usenix UNIX Security Symposium, Baltimore, MD, USA, September 1992.

Bill Cheswick. An evening with Berferd. In Firewalls & Internet Security, chapter 10. Addison-Wesley, Reading, MA, USA, 1994.

53. Un evento, cómo se muestra en la figura siguiente, es la representación de la acción de un *Adversario* que, desplegando una determinada *Capacidad* sobre una *Infraestructura* concreta, ataca a una *Víctima*.

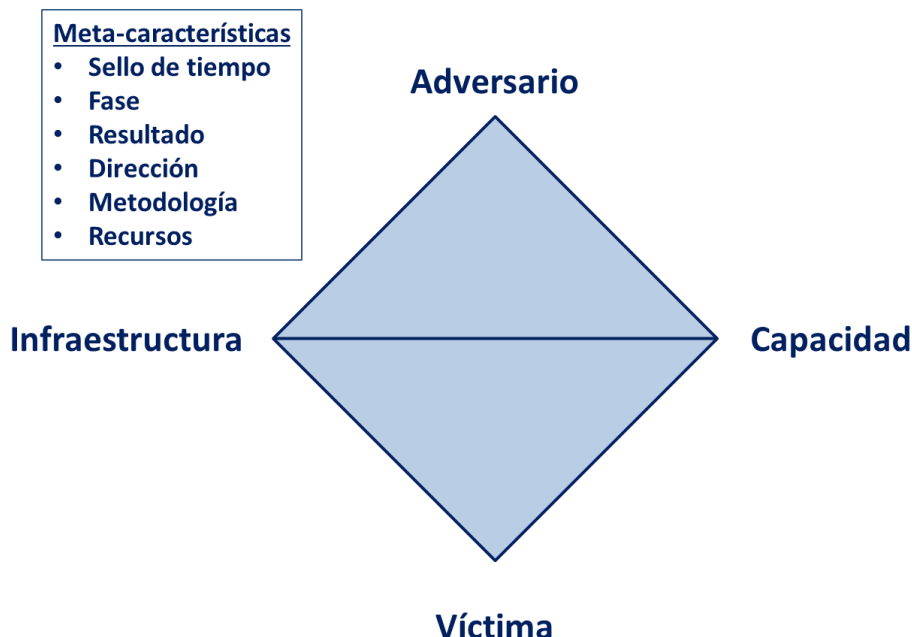


Figura 3: El Evento..

54. **El Evento.** En el Modelo de Diamante para análisis de intrusiones se contemplan las **características principales de un evento de intrusión**: el Adversario, la Capacidad, la Infraestructura y la Víctima. Estas características principales se vinculan a través de aristas para representar sus relaciones fundamentales, que pueden explotarse analíticamente para descubrir y desarrollar el conocimiento de la actividad dañina. La figura incluye **las meta-características** del evento, que, como se verá más adelante, tienen especial importancia en análisis de alto nivel, el estudio de agrupaciones y la planificación de acciones
55. Cuando se ha detectado un evento (intrusión), arranca el proceso de análisis, que consiste en ir dotando de contenido (manual o automáticamente) los vértices (características) del modelo, vinculados por aristas que representan relaciones naturales entre las características enlazadas. Como estudiaremos más adelante, desplazándose entre características, los ciberanalistas pueden deducir información relativa a las operaciones del adversario, pudiendo descubrir nuevas capacidades, infraestructuras o víctimas.
56. Un evento define tan sólo un paso de una serie de ellos que el adversario debe ejecutar para lograr su objetivo. Así pues, los eventos, ordenados en fases y en virtud de una relación concreta adversario-víctima, se configuran en forma de Hilos de Actividad, que representan el flujo de operaciones de un adversario. Ambos, Eventos e Hilos de Actividad constituyen elementos necesarios para lograr comprender la actividad dañina, lo que posibilita una respuesta más eficaz y, como veremos, estratégica¹².

¹² Ver: [11] Eric M. Hutchins, Michael J. Cloppert, and Rohan M. Amin. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. In L. Armistad, editor, International Conference on Information Warfare and Security, volume 6, pages 113–125. Academic Conferences International, Academic Publishing International Unlimited, 2011.

57. Los conceptos y términos mencionados se describen con detalle en los epígrafes siguientes.

3.2. EL EVENTO

Axioma 1: *Para cada Evento existe un Adversario que, persiguiendo un objetivo, haciendo uso de una Capacidad desplegada sobre una Infraestructura, ataca a una Víctima, produciendo un determinado resultado.*

58. Un **Evento** define una actividad limitada en el tiempo y referida a una determinada fase, en la que un *Adversario*, contando con determinados *Recursos*, utilizando una *Capacidad* y una *Metodología* sobre cierta *Infraestructura*, ataca a una *Víctima*, obteniendo un *Resultado* determinado¹³.
59. Los elementos esenciales de un evento son:
- **Características principales:** Las características principales de un evento son: *Adversario*, *Capacidad*, *Infraestructura* y *Víctima*.
 - **Meta-Características:** Las meta-características de un evento son: *Sello de tiempo* (de inicio y de fin), *Fase*, *Resultado*, *Dirección*, *Metodología* y *Recursos*. Las meta-características se utilizan para ordenar los eventos dentro de un *Hilo de Actividad*.
 - **Valor de Confianza:** A cada característica del evento (principal o meta-característica) se le asigna un Valor de Confianza que representa la certidumbre que se otorga al contenido de cada característica.
60. Una de las ventajas del Modelo de Diamante es la de proporcionar una relación de características (no necesariamente exhaustiva) que deben estar presentes en todo evento. Por tanto, si el analista documenta un evento con toda la información que es conocida hasta ese momento, podrá determinar con facilidad cual es la información que falta para caracterizar adecuadamente tal evento.
61. Formalmente, un **Evento**, *E*, se define como un sistema compuesto por cada característica y su valor de confianza, de la forma:

$$\begin{aligned}
 E = & \langle \langle \text{Adversario}, \text{Confianza}_{\text{Adversario}} \rangle, \\
 & \langle \text{Capacidad}, \text{Confianza}_{\text{Capacidad}} \rangle, \\
 & \langle \text{Infraestructura}, \text{Confianza}_{\text{Infraestructura}} \rangle, \\
 & \langle \text{Víctima}, \text{Confianza}_{\text{Víctima}} \rangle, \\
 & \langle \text{Sello de tiempo}_{\text{inicio}}, \text{Confianza}_{\text{Sello de tiempo-inicio}} \rangle, \\
 & \langle \text{Sello de tiempo}_{\text{final}}, \text{Confianza}_{\text{Sello de tiempo-final}} \rangle, \\
 & \langle \text{Fase}, \text{Confianza}_{\text{Fase}} \rangle, \\
 & \langle \text{Resultado}, \text{Confianza}_{\text{Resultado}} \rangle, \\
 & \langle \text{Dirección}, \text{Confianza}_{\text{Dirección}} \rangle,
 \end{aligned}$$

¹³ Obviamente, no es necesario conocer todas las características de un evento para crearlo. Frecuentemente, la mayoría de las características son desconocidas al principio, completándose a medida que se descubren nuevos datos.

$\langle \text{Metodología}, \text{Confianza}_{\text{Metodología}} \rangle,$

$\langle \text{Recursos}, \text{Confianza}_{\text{Recursos}} \rangle \rangle$

62. Al objeto de definir de forma más precisa el conocimiento, cada uno de los anteriores pares puede ampliarse con nuevas sub-características, por ejemplo, para ofrecer más información de la víctima, tal como: Organización, Dirección IP, Nombre del Host, Aplicación atacada y Puerto TCP usado por el atacante, etc., de la forma:

$$\begin{aligned} \langle \text{Víctima}, \text{Confianza}_{\text{Víctima}} \rangle = & \langle \langle \text{Organización}, \text{Confianza}_{\text{Organización}} \rangle, \\ & \langle \text{DirecciónIPHost}, \text{Confianza}_{\text{DirecciónIPHost}} \rangle, \\ & \langle \text{NombreHost}, \text{Confianza}_{\text{NombreHost}} \rangle, \\ & \langle \text{Aplicación}, \text{Confianza}_{\text{Aplicación}} \rangle, \\ & \langle \text{PuertoTCP}, \text{Confianza}_{\text{PuertoTCP}} \rangle \rangle \end{aligned}$$

63. Para el proceso de análisis suele ser útil representar cada evento como el grafo mostrado en la Figura 3 anterior.
64. Las aristas de dicho grafo representan las relaciones naturales entre las características principales del evento. Los vértices y las aristas también puede representarse formalmente, del modo:

$$E_{\text{vértices}} = \{ \text{Adversario}, \text{Infraestructura}, \text{Capacidad}, \text{Víctima} \}$$

$$\begin{aligned} E_{\text{aristas}} = & \{ \{ \text{Adversario}, \text{Capacidad} \}, \\ & \{ \text{Adversario}, \text{Infraestructura} \}, \\ & \{ \text{Infraestructura}, \text{Capacidad} \}, \\ & \{ \text{Infraestructura}, \text{Víctima} \}, \\ & \{ \text{Capacidad}, \text{Víctima} \} \} \end{aligned}$$

3.2.1 EL ADVERSARIO

Axioma 2: Existe un conjunto de adversarios (internos, externos, individuales, grupos y organizaciones) cuya intención es comprometer los sistemas o las redes de sus víctimas, para satisfacer determinadas necesidades.

65. Se denomina **Adversario** a la persona/organización responsable de la utilización de una determinada capacidad contra la víctima, para lograr su propósito. Con frecuencia es difícil conocer la identidad del *Adversario*, lo que hará que, en muchas ocasiones, esta característica del evento no posea contenido, al menos en el mismo momento del descubrimiento de la intrusión.
66. Pueden existir los siguientes tipos de adversarios:
- **Adversario-Operador:** Se trata de la persona o personas que dirigen el ataque.
 - **Adversario-Cliente:** Es la entidad que resulta beneficiada del ataque. Puede ser el mismo Adversario-Operador anterior o puede tratarse de una entidad distinta.

67. El conocimiento de las motivaciones¹⁴ y los recursos de los Adversarios (Operador o Cliente) será de ayuda para determinar la amenaza y el riesgo reales y la mejor forma de mitigarlo.

3.2.2 LA CAPACIDAD

68. La característica de *Capacidad*¹⁵ describe las herramientas o técnicas usadas por el adversario en su intrusión.
69. Pueden distinguirse los siguientes elementos:
- **Sistema de Vulnerabilidades**¹⁶: compuesto por todas las vulnerabilidades que podrían ser explotadas por cada una de las capacidades del adversario, independientemente de la víctima de que trate
 - **Arsenal del Adversario**: El conjunto completo de todas las capacidades de un adversario.
70. Dentro de la Capacidad podemos encuadrar también a los Sistemas de **Mando y Control** (*Command and Control, C2*), que representa el ejercicio de autoridad en el ataque por parte del adversario, y que se compone de canales, estructuras de comunicación, señales, protocolos y determinado contenido con origen o destino en el adversario, dirigido habitualmente a comandar el código dañino introducido en los sistemas de las víctimas, con el objeto de alcanzar el objetivo perseguido.
71. La figura siguiente muestra un esquema de estos conceptos y su relación.

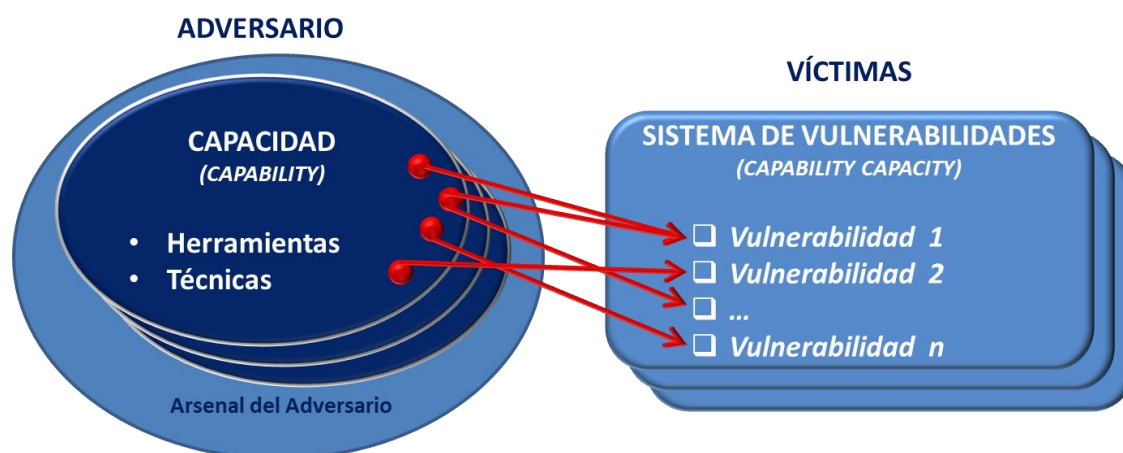


Figura 4: La *Capacidad* del adversario

3.2.3 LA INFRAESTRUCTURA

72. La característica *Infraestructura* comprende las estructuras físicas y/o lógicas de comunicación que *Adversario* utiliza para desplegar su *Capacidad*, mantener el control de la misma (mediante sistemas de Mando y Control (C2), por ejemplo) y asegurar los resultados esperados en la *Víctima* (exfiltración de datos, por ejemplo). Al igual que el resto de las características del evento, la *Infraestructura* puede ampliarse con nuevas sub-

¹⁴ Como veremos más adelante, las motivaciones pueden ser de muchas clases: económicas, sociales, políticas, militares, etc.

¹⁵ A la que suele denominarse como *Capability*, en la bibliografía anglosajona.

¹⁶ A la que suele denominarse como *Capability Capacity*, en la bibliografía anglosajona.

características, tales como: Protocolo de Internet (*Internet Protocol*, IP), Nombres de Dominio, Direcciones de correo electrónico, tarjetas de memoria USB o pendrives, emanaciones del hardware, etc.

73. Podemos clasificar las infraestructuras en los siguientes tipos:

- **Infraestructura Tipo 1:** Aquella que el adversario controla totalmente, le pertenece o se encuentra en su inmediatez física.
- **Infraestructura Tipo 2:** Aquella que controla un intermediario (deliberada o involuntariamente). Se trata de un tipo de infraestructura que la víctima consideraría su adversario, ocultando su verdadero origen y, por tanto, dificultando la atribución de la intrusión. Son ejemplos: ordenadores infectados controlados remotamente (host zombis), servidores de código malicioso (malware), nombres de dominio dañinos, cuentas de correo electrónico comprometidas, etc.
- **Proveedores de Servicios:** Aquellas organizaciones que (deliberada o involuntariamente) proporcionan servicios esenciales para asegurar la disponibilidad de las infraestructuras (Tipo 1 o Tipo 2) del adversario, tales como: Proveedores de Servicios de Internet, registradores de dominio, Proveedores de correo-web, etc.

3.2.4 LA VÍCTIMA

84. La *Víctima* constituye el objetivo del *Adversario*, atacando sus vulnerabilidades haciendo uso de sus *Capacidades*¹⁷. De forma análoga a lo que sucede con otras características del evento, una víctima puede describirse con la profundidad que se estime necesaria: Organización, persona física, correo electrónico objetivo, dirección IP, nombre de dominio, etc. Esto resulta especialmente útil cuando al análisis se aplican técnicas de victimología y acercamientos de tipo socio-político.

85. Podemos establecer los siguientes tipos de víctimas:

- **Víctima-Persona:** Pueden serlo tanto personas físicas como organizaciones, incluyendo nombres, razones sociales, industrias, cargos o puestos de trabajo, intereses, etc.
- **Víctima-Activo:** Lo constituye toda la superficie de ataque de la víctima y comprende el conjunto de redes, sistemas, hosts, direcciones de email, direcciones IP, cuentas de redes sociales, alojamientos en la nube, etc., contra las que el adversario despliega sus capacidades. Una Víctima-Activo puede ser el objetivo final o puede formar parte de la infraestructura en ataques posteriores.

Axioma 3: *Cada sistema y, por extensión, cada activo de la víctima, tiene vulnerabilidades o exposiciones.*

84. Se denominan ***Brechas Vulnerables de la Víctima*** al conjunto de vulnerabilidades y exposiciones de la víctima susceptibles de ser explotadas por un adversario.

85. De manera análoga a lo que sucede con otras características del modelo, cada una de las vulnerabilidades, de cada uno de los elementos que componen su superficie de ataque, puede expresarse como un nuevo par de la forma

$\langle \text{Víctima}, \text{Activo}_{\text{Vulnerabilidad}} \rangle$

¹⁷ Ver: MITRE. Common vulnerabilities and exposures. <http://cve.mitre.org/>

3.2.5 LAS META-CARACTERÍSTICAS

86. Las meta-características se utilizan para incluir en el evento otras características adicionales no-críticas, pero que pueden resultar importantes durante el análisis.

87. Son las siguientes:

- **Sello de tiempo:** Fecha/hora de inicio y final del evento, lo que podría permitir el análisis de patrones de comportamiento del adversario, periodicidad o recurrencia de los ataques, etc.
- **Fase:** Una actividad dañina no consta de un único evento, sino que, por el contrario, debe constar de dos o más eventos que el atacante desarrolla sucesivamente. Es lo que se ha dado en llamar *cadena de eventos*¹⁸.

Axioma 4: *Cada actividad intrusiva contiene dos o más fases que el adversario acomete sucesivamente, al objeto de lograr el objetivo perseguido.*

La fase de un evento determina su localización en el *Hilo de Actividad* del ataque.

Formalmente, las fases F se definen como un sistema del tipo:

$$F = \langle f_1, f_2, \dots, f_n \rangle$$

Dónde:

$n \geq 2$ (existen, al menos, dos fases en cada ataque).

f es una fase en la cadena de operaciones del adversario.

f_1 es la primera fase de las acciones del adversario.

- **Resultado:** Es la utilidad particular que el adversario persigue cuando ataca a la víctima. Suele ser de tal naturaleza que, a priori, no es fácil conocer si el ataque ha tenido o no éxito, desde el punto de vista del adversario. Por este motivo, puede completarse esta característica con una indicación de su resultado, del tipo:

<Éxito, Fracaso, Desconocido>

Otra forma de caracterizar el resultado del evento es señalar la dimensión o dimensiones de la seguridad que se han visto comprometidas: *Confidencialidad, Integridad o Disponibilidad*¹⁹.

Naturalmente, la flexibilidad del modelo permite incluir más elementos caracterizadores del resultado de la acción del adversario: tipo de información comprometida, etc.²⁰

- **Dirección:** La dirección del ataque resulta un elemento importante cuando se considera la posibilidad de adoptar medidas de mitigación, especialmente en los eventos basados en red. Esta meta-característica puede tomar uno de los siete valores siguientes: *Víctima-a-Infraestructura, Infraestructura-a-Víctima, Infraestructura-a-*

¹⁸ Por ejemplo, un adversario debe: 1. Localizar la víctima de su ataque, 2. Descubrir una vulnerabilidad, 3.

Desarrollar un instrumento que explote la vulnerabilidad, 4. Atacar tal vulnerabilidad, 5. Comunicar con el C2, etc.

¹⁹ A las que habría que añadir *Trazabilidad y Autenticidad*, en los sistemas del ámbito de aplicación del Esquema Nacional de Seguridad.

²⁰ Ver: Frederick B. Cohen. *Protection and Security on the Information Superhighway*. John Wiley & Sons, New York, NY, USA, 1995.

Infraestructura, Adversario-a-Infraestructura, Infraestructura-a-Adversario, Bidireccional o Desconocido.

- **Metodología:** La meta-característica *Metodología* posibilita al analista describir el tipo de actividad desarrollada por el adversario, tal como: correos electrónicos con suplantación de identidad (email con *spear-phishing*), ataque de denegación de servicio por inundación del sistema de peticiones de conexión (*syn flood*), escaneo de puertos, etc. Análogamente a lo que sucede con otras características, esta puede ampliarse con distintos tipos, por ejemplo: (*spear-phishing* email – con contenido malicioso), (*spear-phishing* email – enlace malicioso), etc. Esta característica permite categorizar mejor los eventos y posibilita la comparación de indicadores independientes, aplicables a uno sólo o a una agrupación de adversarios.

Algunas taxonomías ampliamente conocidas pueden incorporarse a esta característica²¹.

- **Recursos:** La meta-característica *Recursos* comprende el conjunto de recursos externos de que es necesario disponer para asegurar el resultado del evento.

Axioma 5: *Cada evento de intrusión requiere previamente de uno o más recursos externos para alcanzar el éxito.*

Los Recursos deben entenderse en sentido amplio²² y constituyen elementos especialmente importantes cuando se consideran estrategias de mitigación centradas en esta característica o durante la identificación de lagunas de conocimiento y/o comprobación de hipótesis, como estudiaremos más adelante.

Algunos ejemplos de Recursos son:

- Software (por ejemplo: metasploit, sistemas operativos, software de virtualización, etc.)
- Conocimiento (por ejemplo: cómo ejecutar metasploit, dónde obtener exploits, etc.)
- Información (por ejemplo: un nombre de usuario/contraseña supuesta, etc.)
- Hardware (por ejemplo: estaciones de trabajo, servidores, módems, etc.)
- Recursos económicos (por ejemplo: para la compra de dominios, etc.)
- Instalaciones (por ejemplo: electricidad, contenedores, etc.)
- Acceso (por ejemplo: un enlace desde el host origen a la víctima y viceversa, una dirección IP, acceso a la red de un proveedor de servicios de Internet, etc.)
- **Características adicionales:** Además de las características principales, pueden considerarse otras características de un evento de intrusión que podrían tener especial importancia para atender las necesidades de una organización concreta, tales como: la *f fuente de datos* (que detectó el evento), el *autor* (el analista-autor del evento), el *método de detección* (la herramienta, la técnica o la capacidad que detectó el evento dañino), la *firma de la detección* (firma o heurístico detectado en el evento), etc. El uso de este tipo de características mejora la eficacia del modelo, permitiendo a

²¹ Tales como las llamadas “clases Snort”. Snort Users Manual 2.9.3, pág. 179. The Snort Project, May 2012.

²² Obviamente, esta meta-característica puede abarcar una inmensa cantidad de elementos. Sin embargo, como con el resto de características del modelo, no es necesaria completitud sino solamente suficiencia. Por lo tanto, una organización sólo tendría que tomar en consideración aquellos recursos necesarios para la aplicación del modelo en su propia organización.

usuarios, analistas, y organizaciones conservar para un uso futuro información significativa asociada al evento en cuestión.

3.3. EXTENSIÓN DEL MODELO

84. Además de las características principales, el Modelo de Diamante puede ampliar su funcionalidad incorporando nuevas características, con el objetivo de lograr una mejor definición de los eventos y, en su consecuencia, la conducta de los adversarios.
85. Así, podemos incluir dos nuevas meta-características: la **Socio-Política**, que vincula al *Adversario* con su *Víctima* y la **Tecnológica**, que vincula a la *Infraestructura* con la *Capacidad*, tal y como se representa en la figura siguiente.

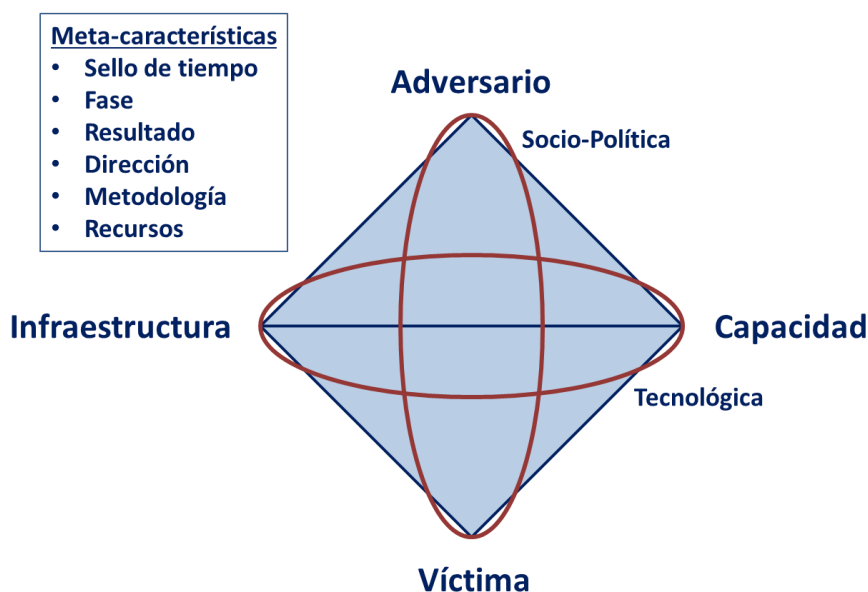


Figura 5: El modelo puede extenderse con nuevas características.

86. El modelo puede extenderse con nuevas características. En este caso se muestra la característica Socio-Política que enlaza al Adversario con su Víctima (para recoger las necesidades socio-políticas, aspiraciones y motivos del adversario y la disponibilidad de la víctima de satisfacer tales necesidades), y la característica Tecnológica, que enlaza la Capacidad usada por el adversario con la Infraestructura sobre la que se despliega (para recoger datos sobre la tecnología que posibilita la relación anterior).

3.3.1 LA CARACTERÍSTICA SOCIO-POLÍTICA

Axioma 6: Siempre existe una relación entre el Adversario y su Víctima, aunque tal relación pueda ser distante, fugaz o indirecta.

87. El vínculo *Adversario-Víctima* se basa en una relación productor-consumidor, sustentada en las necesidades y aspiraciones socio-políticas del adversario (generar ingresos, lograr la aceptación en una determinada comunidad, aumentar los beneficios empresariales, obtener información valiosa, etc.). Esta relación comprende tanto las necesidades del adversario-consumidor como la capacidad de la víctima-productor para satisfacer aquellas necesidades, de modo directo (materialización de ciberespionaje, ciberdelito, etc.) o indirecto (recursos informáticos para despliegue de una red de equipos infectados por un atacante remoto (*botnets*), ataques por denegación de servicio, etc.).

88. **La intención:** Aunque la *intención* es un aspecto esencial para analizar las intrusiones, ayudando a adoptar las decisiones de mitigación más oportunas, no constituye en sí misma una característica principal del evento, encontrando mejor encaje dentro de la meta-característica Socio-Política.
89. No todas las relaciones *Adversario-Víctima* son iguales. Algunos adversarios desarrollan sus ataques sin ambicionar más de lo que son capaces de lograr de forma inmediata, sin temor a perder el acceso al sistema atacado. Otros, sin embargo, persiguen permanecer inadvertidos el mayor tiempo posible (frecuente en los casos de ciberespionaje, por ejemplo) o, incluso, tomar represalias si la víctima decide hacerles frente.
90. La persistencia del adversario, por consiguiente, constituye un elemento de la máxima importancia para caracterizar la relación *Adversario-Víctima*.

Axioma 7: *Existe un subconjunto del conjunto de adversarios que posee la motivación, los recursos y las capacidades para mantener sus ataques dirigidos contra una o más víctimas durante un significativo periodo de tiempo, a pesar de los esfuerzos de mitigación de las víctimas.*

91. Este tipo de relación es la que se ha venido evidenciando de manera práctica en las llamadas **APT** (**Advanced Persistent Threats**, Amenazas Persistentes Avanzadas) que constituyen actualmente la variante más peligrosa de los vectores de ataque, destinados, por lo común, al ciberespionaje y, últimamente, también al ciberdelito.
92. **Adversario Persistente:** Un adversario persistente es un adversario que satisface el axioma 7, dentro de una relación *Adversario-Víctima* concreta.
93. Como es lógico suponer, que un adversario sea persistente con una víctima concreta no significa que lo sea con todas sus posibles víctimas. Su comportamiento dependerá del interés que le mueva a atacar a la víctima concreta y los resultados que espera obtener si sus acciones tienen éxito.
94. Análogamente, una misma víctima puede tener adversarios que sean persistentes y otros que no lo sean. En conclusión: la persistencia o no persistencia viene determinada por el par *Adversario-Víctima* de que se trate en cada momento²³.
95. El **grado de persistencia** denota la fortaleza de los motivos del adversario, sus capacidades y los recursos que debe utilizar para mantener el efecto deseado.

Corolario 1: *Existen varios grados de persistencia del adversario sustentados en la esencia de la relación concreta Adversario-Víctima.*

96. Haciendo de la meta-característica *Socio-Política*, sus necesidades y aspiraciones asociadas, una parte clave de la actividad dañina, el Modelo de Diamante permite la aplicación al análisis de áreas de conocimiento no tradicionales, tales como la psicología, la criminología, la victimología, el marketing, el comportamiento del consumidor y la economía, todo ello de cara a ampliar las opciones de mitigación.
97. Los siguientes constituyen algunos de los elementos de la relación *Adversario-Víctima* que podrían determinar el grado de persistencia:

²³ Ver: Clifford Stoll. Stalking the wily hacker. Communications of the ACM, 31(5):484–497, May 1988; y Bill Cheswick. An evening with Berferd. In Firewalls & Internet Security, chapter 10. Addison-Wesley, Reading, MA, USA, 1994.

- La solidez de aquellas necesidades del adversario que pueden ser satisfechas por la víctima.
 - El riesgo que el adversario percibe en relación con sus acciones.
 - El coste que el adversario debe asumir para mantener sus acciones.
 - La singularidad de la víctima para satisfacer una necesidad determinada y su inmanencia en el tiempo.
 - El nivel de esfuerzo y recursos requeridos para resistir a la persistencia.
98. Las consideraciones anteriores nos llevan a definir los siguientes dos tipos de víctima:
- **Víctima de Oportunidad**: es aquella que representa una *commodity* para las operaciones del adversario: es decir, se trata de una víctima reemplazable. Si el adversario perdiera el acceso a la misma no es probable que consumiera recursos para obtener de nuevo tal acceso. Debido a su disponibilidad y vulnerabilidades, este tipo de víctimas, frecuentemente, suelen ser las primeras en recibir los ataques.
 - **Víctima de Interés**: se trata de aquella que no es reemplazable para el adversario puesto que espera obtener de ella un valor permanente. Si el adversario perdiera su acceso, intentaría recuperarlo.
99. Frecuentemente, una relación *Adversario-Víctima* no permanece estática sino que, por el contrario, suele incrementarse en el tiempo, si se dan las condiciones oportunas para ello. Este sería el caso de la transformación de una víctima, de Víctima de Oportunidad a Víctima de Interés, cuando el adversario, una vez accedida, comprueba que posee información de especial importancia para él.
100. Puesto que el Modelo de Diamante puede ampliarse incorporando varios adversarios y/o víctimas a través de lo que más adelante definiremos como *Hilos de Actividad* y *Grupos de Actividad*, pueden desarrollarse toda clase de analíticas relacionadas con la criminología y la victimología, capaces de dar respuesta a preguntas tales como:
- ¿Por qué una entidad concreta ha sido víctima de un ataque?
 - ¿Hay un conjunto común de víctimas?
 - ¿Han compartido las víctimas un tratamiento común?
 - ¿Puede deducirse la intención del adversario del conjunto de víctimas atacado?
 - ¿Quiénes podrían resultar ser otras víctimas?
 - ¿Quién ha tenido la necesidad y la intención de hacer víctimas a tal conjunto de organizaciones?
101. Disponiendo de un buen modelo de análisis victimológico, pueden examinarse métodos para contrarrestar las acciones de los adversarios, haciendo que las víctimas aparezcan como menos atractivas o, incluso, predecir víctimas futuras²⁴.

²⁴ Los más recientes ataques por “watering-hole” ilustran cómo los adversarios pueden usar estos conceptos para perfilar a sus víctimas y colocar sus exploits (programas maliciosos que explotan una vulnerabilidad) en los lugares que les reporten mayores beneficios. Si la característica Socio-Política se usa de forma eficaz, con una aproximación centrada en la víctima, se pueden predecir muchas de las ubicaciones en las que los atacantes colocarán sus exploits de “watering-hole”, facilitando la instalación de las medidas de seguridad adecuadas en tales sitios.

102. Finalmente, si dos o más víctimas comparten suficientes características que podrían satisfacer las necesidades de uno o más adversarios, nos encontramos en lo que se ha denominado un *espacio de amenazas compartido*. La identificación temprana de tales superficies constituye una piedra angular para acciones estratégicas de mitigación proactiva²⁵.
103. Por este motivo, compartir inteligencia de amenazas constituye una estrategia muy eficaz, especialmente entre aquellas organizaciones que podrían resultar víctimas similares para los adversarios.

3.3.2 LA CARACTERÍSTICA TECNOLÓGICA

104. Como hemos dicho, la meta-característica *Tecnológica* relaciona dos características principales: *Capacidad* e *Infraestructura*.²⁶
105. Analizando la tecnología usada y sus peculiaridades, un analista puede descubrir una nueva actividad dañina independientemente de la Infraestructura y la Capacidad subyacentes. Más aún, comprender las tecnologías involucradas en la actividad de un adversario facilita la identificación de los lugares de detección más apropiados, los tipos de datos y las capacidades.

3.4. INDICADORES DE CONTEXTO

106. Se denominan **Indicadores** aquellos elementos de información usados por los sistemas y los analistas para detectar las operaciones del adversario y sus características.
107. Aunque, tradicionalmente, los indicadores se han venido correspondiendo con la aportación de datos de naturaleza técnica, en la actualidad, tales indicadores se corresponden también con aspectos no-técnicos aunque su implementación automática no sea siempre posible.
108. **Indicador de contexto**: un indicador de contexto es un elemento de información situado en el contexto de las operaciones de un adversario, que refuerza las operaciones de detección y análisis. Los indicadores de contexto aseguran la obtención de la información necesaria para el análisis y su posterior tratamiento.
109. Usando los indicadores de contexto, el proceso de análisis está en condiciones no sólo de detectar y confirmar la intrusión (alcanzables usando indicadores tradicionales) sino también determinar si tal intrusión pertenece a una campaña del adversario, la información perseguida en su ataque, su intención y las potenciales necesidades socio-políticas que podrían perseguir las operaciones de futuros adversarios.
110. Obviamente, el uso de estas herramientas permite a la organización-víctima adoptar medidas de mitigación más eficaces.

3.5. ANÁLISIS DIRIGIDO

111. Entenderemos por *análisis dirigido* la técnica usada para obtener un elemento de información y explotarlo adecuadamente, al objeto de descubrir elementos relacionados. En último extremo, el análisis dirigido constituye un mecanismo de prueba y verificación

²⁵ Por ejemplo, ataques dirigidos contra un miembro de un determinado colectivo pueden predecir posibles ataques a otros miembros que compartan su ecosistema.

²⁶ Por ejemplo, si un código dañino es capaz de resolver dominios y comunicarse a través de HTTP, las tecnologías usadas serían: Internet Protocol (IP), Transport Control Protocol (TCP), Hypertext Transport Protocol (HTTP) y el sistema de nombres de dominio Domain Name System (DNS).

de hipótesis, donde cada elemento de un evento de intrusión podría generar sus propias hipótesis, que requerirían de posteriores evidencias que condujeran a su afirmación, negación o modificación.

112. En resumen, el análisis dirigido es la actividad tendente a descubrir elementos relacionados (evidencias) capaces tanto de sustentar una hipótesis previa como generar nuevas hipótesis.

113. La capacidad de análisis dirigido es una de las fortalezas del Modelo de Diamante. El analista, partiendo de un punto del modelo (vértice) podría estar en condiciones de descubrir y desarrollar otras características que estuvieren conectadas, aunque no se pueda garantizar el éxito en todos los casos.

114. La figura siguiente muestra un ejemplo de este tipo de análisis.

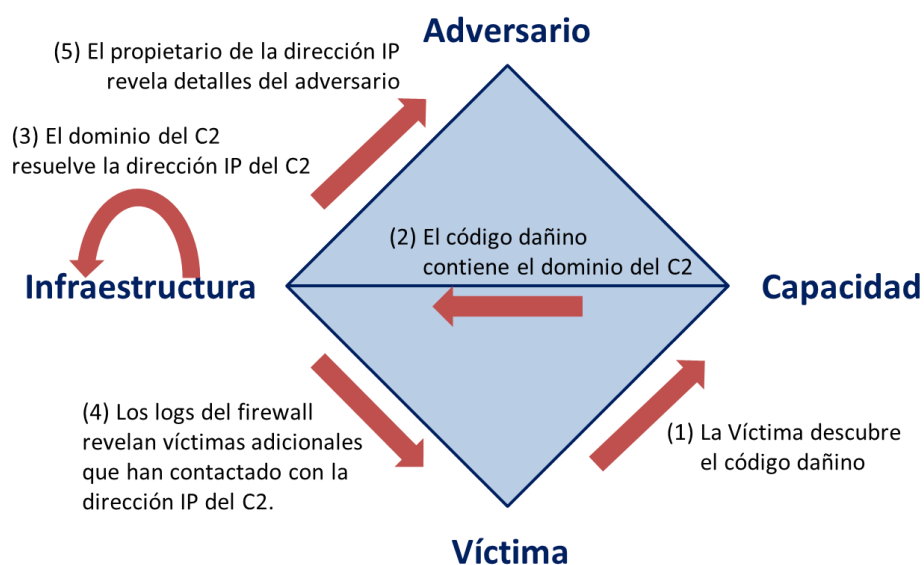


Figura 6: Ejemplo de análisis dirigido.

115. En la figura anterior, el proceso de análisis dirigido ha seguido los siguientes pasos:

- (Paso 1): La víctima descubre código dañino en su red.
- (Paso 2): El código dañino se pone en contacto con el dominio de su centro de mando y control (C2).
- (Paso 3): El dominio es resuelto, evidenciando la dirección IP que aloja el controlador de código dañino.
- (Paso 4): Se examinan los registros del cortafuegos (logs del firewall), descubriéndose otros equipos hosts comprometidos en la red de la víctima, que hubieran establecido comunicaciones con la dirección IP recientemente descubierta.
- (Paso 5): El registro de la dirección IP revela detalles adicionales que permiten la atribución de la autoría.

3.5.1 ORIGEN DEL ANÁLISIS

116. El Modelo de Diamante permite seleccionar el origen del proceso de análisis (vértice-característica), lo que, como decimos, posibilita no sólo descubrir nueva actividad dañina,

sino revelar actividad relacionada con otras características conectadas o con la propia característica de arranque. Seguidamente, se examinan los posibles orígenes del análisis.

117. **La Víctima como origen del análisis:** el análisis de datos de una potencial víctima revela otros elementos relacionados, conectados a través de las aristas del evento: las capacidades del adversario y la infraestructura sobre la que se despliegan²⁷.
118. **La Capacidad como origen del análisis:** en este tipo de análisis se explota las características de la capacidad para descubrir otros elementos relacionados en las operaciones del adversario: las víctimas contra las que puede ser usada tal capacidad, la infraestructura que la soporta, la tecnología que la permite, pistas sobre otras características relacionadas y, posiblemente, pistas sobre el adversario²⁸.
119. **La Infraestructura como origen del análisis:** en este análisis se pone el foco en la infraestructura dañina del adversario. Partiendo de este elemento pueden descubrirse otros relacionados: víctimas en contacto o con la misma infraestructura, capacidades desarrolladas o controladas por la infraestructura, otras infraestructuras relacionadas (tales como direcciones IP resueltas por dominios dañinos) y, posiblemente, pistas del adversario, incluyendo aquellos que pudieran controlar directamente la infraestructura en estudio²⁹.
120. **El Adversario como origen del análisis:** este tipo de análisis implica la monitorización del adversario al objeto descubrir sus capacidades y las infraestructuras sobre las que son desplegadas. Obviamente, aun tratándose de la aproximación potencialmente más provechosa, está limitada a la necesidad de tener acceso a los sistemas usados por el atacante³⁰.
121. **La característica Socio-Política como origen del análisis:** este tipo de análisis no conduce directamente a la obtención de nuevos elementos o indicadores, sino que se fundamenta en una supuesta relación adversario-víctima sobre la que se pretende construir hipótesis relativas a la identificación de posibles adversarios y sus posibles víctimas. Los resultados obtenidos en este procedimiento podrían usarse para acometer nuevos análisis

²⁷ El proyecto Honeynet Project es un buen ejemplo de este tipo de análisis. Lance Spitzer. The honeynet project: Trapping the hackers. Security & Privacy, page 15, April 2003.

²⁸ Algunos ejemplos de este modelo de análisis es el desarrollado para Stuxnet y Duqu por Symantec y CrySys, y sustentado en el análisis de varias características y técnicas comunes empleadas en ambos códigos. Otro ejemplo puede ser el análisis de Red October, desarrollado por Kaspersky.

Ver: Symantec Security Response. W32.Duqu: The precursor to the next Stuxnet.

http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf, November 2011 y Red October: Diplomatic cyber attacks investigation.

http://www.securelist.com/en/analysis/204792262/Red_October_Cyber_Attacks_Investigation, 2013.

²⁹ Un ejemplo de este tipo de análisis es el desarrollado por The Command Five Team en sus investigaciones SKHack. Command Five Pty Ltd. SK Hack by an advanced persistent threat.

http://www.commandfive.com/papers/C5_APT_SKHack.pdf, September 2011.

³⁰ Un ejemplo de este tipo de análisis lo encontramos en las actividades del FBI en el curso de la acción

“Phonemasters”, operación en la que la agencia norteamericana consiguió penetrar los sistemas del adversario. Ver D. Ian Hopper and Richard Stenger. Large-scale phone invasion goes unnoticed by all but FBI. CNN, December 1999. <http://edition.cnn.com/1999/TECH/computing/12/14/phone.hacking/> y Nate Anderson. How one man tracked down Anonymous – and paid a heavy price. Ars Technica, February 2011. <http://www.arstechnica.com/tech-policy/2011/02/how-one-security-firm-tracked-anonymousand-paid-a-heavy-price/>

tomando al adversario o a la víctima como origen, tal y como se ha señalado en los párrafos anteriores³¹.

122. **La característica Tecnológica como origen del análisis:** el análisis con origen en la meta-característica *Tecnológica* permite al analista tomar en consideración un uso inusual de la tecnología, al objeto de descubrir infraestructuras o capacidades, hasta entonces desconocidas, que pudieran hacer uso de tal tecnología. La monitorización y detección de anomalías en el DNS ha venido constituyendo un método muy eficaz para desarrollar este tipo de análisis y descubrir actividad dañina nueva³².

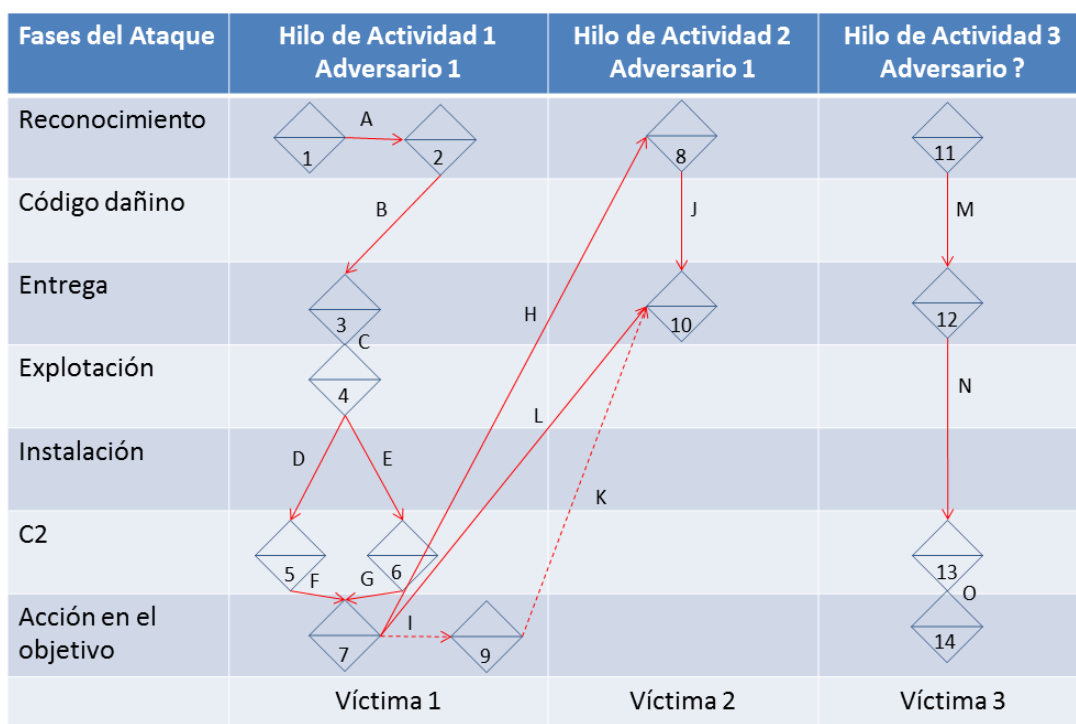
3.6. LOS HILOS DE ACTIVIDAD

123. Como se ha mencionado, la actividad que el adversario dirige contra su víctima no se desarrolla en un único evento sino que, por el contrario, se compone de una cadena de eventos causales, que comprenden un conjunto ordenado de fases en las que, generalmente, cada fase debe ejecutarse satisfactoriamente para alcanzar el objetivo final.
124. Dentro de nuestro modelo se denomina **Hilo de Actividad** a un grafo orientado de fases, donde cada nodo es un evento y los arcos identifican relaciones causales entre tales eventos. Para potenciar la fiabilidad de los análisis realizados con el modelo, los arcos están etiquetados con el grado de confianza que denota la fiabilidad con la que un evento trae causa directa del precedente. Además, la estructura del grafo permite incorporar operadores del tipo AND, para representar caminos necesarios y OR, para representar caminos opcionales.
125. Los Hilos de Actividad se representan verticalmente, señalando cada uno de los eventos causales (ordenados) que ejecuta un adversario contra una víctima concreta. Por tanto, cada hilo se refiere a un determinado par adversario-víctima.
126. La figura siguiente muestra un ejemplo de Hilos de Actividad que relacionan eventos enlazados verticalmente (y que se corresponden con una víctima concreta) y horizontalmente (entre víctimas). Las líneas continuas representan elementos de información soportados por evidencias reales y las líneas discontinuas representan hipótesis.

³¹ Ver: Jose Nazario. Georgia DDoS attacks – a quick summary of observations.

<http://ddos.arbornetworks.com/2008/08/georgia-ddos-attacks-a-quick-summary-of-observations>, August 2008; y Brian Krebs. Cyber attacks target pro-Tibet groups. Washington Post, March. 2008. <http://www.washingtonpost.com/wp-dyn/content/article/2008/03/21/AR2008032102605.html>.

³² Ver: Bojan Zdrnja, Nevil Brownlee, and Duane Wessels. Passive monitoring of DNS anomalies. In Proceedings of the 4th International Conference on Detection of Intrusions and Malware and Vulnerability Assessments, DIMVA '07, pages 129–139, Berlin, Heidelberg, 2007. Springer-Verlag; Manos Antonakakis, Roberto Perdisci, Wenke Lee, Nikolas Vasiloglou, II, and David Dagon. Detecting malware domains at the upper DNS hierarchy. In Proceedings of the 20th USENIX Conference on Security, SEC'11, pages 27–27, Berkeley, CA, USA, 2011. USENIX Association; y Wolfgang John and Tomas Olovsson. Detection of malicious traffic on back-bone links via packet header analysis. Campus-Wide Information Systems, (25):342–358, 2008.

Figura 7: Ejemplo de *Hilos de Actividad*

127. La tabla siguiente describe los eventos de la figura 7 anterior.

Evento	Hipótesis / Real	Descripción
1	Real	El Adversario 1 busca en la red información de la empresa Productos Frutícolas, S.A., encontrando que tal empresa tiene registrado el dominio www.dehigosabrevas.com
2	Real	El Adversario 1 usa el dominio hallado para buscar en la red “administrador de red de dehigosabrevas.com”, encontrando que algunos usuarios de ciertos foros se autodenominan así, incluyendo su dirección de correo electrónico.
3	Real	El Adversario 1 remite correos electrónicos de spear-phishing a la dirección anterior, conteniendo un adjunto que contiene un troyano.
4	Real	Un administrador de red de Productos Frutícolas, S.A. (AR1) abre el adjunto, provocando la ejecución del código dañino.
5	Real	El sistema de AR1 atacado envía un mensaje Post HTTP a la dirección IP en la que se encuentra el Centro de Mando y Control (C2) del Adversario 1, que acusa recibo de la transmisión.
6	Real	Mediante ingeniería inversa se descubre el código dañino, que muestra una dirección IP adicional, que parece ser la dirección de respaldo si la primera no responde.
7	Real	A través de un mensaje de respuesta HTTP enviado al host de AR1, el código dañino arranca las conexiones con el proxy TCP.
8	Real	A través del proxy establecido en el sistema de AR1, el Adversario 1 realiza una búsqueda en la red con el argumento “una nueva variedad, más rentable”, encontrando entre los resultados a la

		empresa Investigaciones Frutícolas, S.A.
9	Hipótesis	El Adversario1 verifica la lista de contactos de correo de AR1, buscando aquellos que pudieran ser de Investigaciones Frutícolas, S.A., descubriendo la dirección de correo electrónico de su Director de Investigaciones.
10	Real	El Director de Investigaciones de Investigaciones Frutícolas, S.A. recibe un correo spear-phishing de AR1 de Productos Frutícolas, S.A., incluyendo un adjunto con el mismo código dañino anterior.
11	Real	Un Adversario desconocido explora la web en busca de web servers vulnerables, incluyendo a Víctima 3.
12	Real	Un exploit para una vulnerabilidad se remite a la Víctima 3.
13	Real	El servidor atacado de Víctima 3 establece una conexión remota con el Adversario.
14	Real	El Adversario usa la conexión remota para descargar los documentos de en el directorio privado de Víctima 3.

128.La tabla siguiente describe los arcos de la figura 7.

Arco	Confianza	AND/OR	Hipótesis/Real	Proporciona
A	Baja	AND	Real	Proporciona el dominio para Productos Frutícolas, S.A. (www.dehigosabrevas.com)
B	Alta	AND	Real	Proporciona los objetivos del spear-phishing: direcciones de correo electrónico de los administradores de red de www.dehigosabrevas.com
C	Alta	AND	Real	Ninguno
D	Alta	OR	Real	Ninguno
E	Alta	OR	Real	Ninguno
F	Alta	AND	Real	Ninguno
G	Alta	AND	Real	Ninguno
H	Media	AND	Real	Proporciona acceso proxy desde víctima anterior al motor de búsqueda.
I	Baja	AND	Hipótesis	Acceso a la lista de contactos.
J	Alta	AND	Real	Identificación de la organización de la víctima.
K	Baja	AND	Hipótesis	Dirección de correo electrónico, nombre e identificación del rol de la víctima.
L	Alta	AND	Real	Correo electrónico de spear-phishing troyanizado.
M	Alta	AND	Real	Proporciona los resultados satisfactorios del análisis que identifica el servidor web de la víctima como vulnerable al ataque.
N	Alta	AND	Real	Ninguno
O	Alta	AND	Real	Proporciona el establecimiento de la conexión remota.

129. Así las cosas, podemos definir los siguientes conceptos:
130. **Correlación Vertical**: se trata del proceso de análisis de identificación de brechas de conocimiento, completando tales brechas con nuevos conocimientos, y estableciendo relaciones causales (con sus correspondientes etiquetas de confianza) dentro de un Hilo de Actividad vertical de la relación Adversario-Víctima.
131. **Correlación Horizontal**: se trata del proceso de análisis de causalidad que enlaza eventos entre Hilos de Actividad vertical, a través de los pares adversario-víctima, identificando brechas ya conocidas entre Hilos de Actividad y usando el conocimiento de un Hilo para completar las brechas de conocimiento de otro.
132. Sea como fuere, los Hilos de Actividad conforman un nuevo tipo de grafo de ataque orientado a través de fases, formado a partir de observaciones de eventos reales, para predecir la probabilidad o preferencia de un adversario para adoptar un determinado camino de ataque.
133. Formalmente, puede definirse un Hilo de Actividad como un grafo dirigido **HA**, donde:

$HA = (V, A)$ es un par ordenado, tal que:

$|V| \geq 1$. Es decir, existe al menos un evento en cada Hilo de Actividad,

HA es un grafo finito,

V es el conjunto de todos los eventos, clasificados en subconjuntos, tal que todos los eventos de un subconjunto comparten los mismos adversarios y víctimas, y están divididos en un conjunto de p tuplas etiquetadas, donde p es el número de fases definidas.

A es el conjunto ordenado de pares de arcos, tal que $arc(x, y)$ se encuentra definido si y sólo si el adversario ejecuta con éxito el evento y porque el evento x precede inmediatamente al evento y .

Puede existir más de un arco desde o a cualquier evento.

Sólo existe un camino de un nodo a otro.

Los arcos están etiquetados con una tupla del tipo: $\langle \text{Confianza}, \text{AND/OR}, \text{Hipótesis/Real}, \text{Proporciona} \rangle$, donde:

- *Confianza*, define la confianza analítica en la existencia de una relación causal entre x e y .
- *AND/OR*, define si el camino desde x hasta y es necesario (AND) o se trata de un camino opcional (OR).
- *Hipótesis/Real*, distingue un arco hipotético de un arco real.
- *Proporciona*, define los recursos que x proporciona a y para que concuerden con los requerimientos recogidos en la meta-característica *Recursos* del evento.

3.6.1 EL PROCESO DEL ADVERSARIO

134. Globalmente considerados, los Hilos de Actividad verticales y los enlaces horizontales describen el proceso (de ataque) de un adversario, de principio a fin. La información de este proceso se enriquece, además, con las características de cada una de las acciones individuales que lo componen (eventos). Así, de forma conjunta, ambos (Hilos de Actividad y eventos) definen CÓMO ejecuta sus acciones el adversario, es decir, su *modus operandi*.

135. Por otro lado, como quiera que en muchas ocasiones un adversario puede sentir preferencia por ciertos elementos o comportamientos concretos, el análisis de intrusión debe identificar esas preferencias, analizando los elementos que pudieran tener en común cada una de las campañas realizadas por el atacante. La capacidad para identificar y articular estas características y comportamientos comunes constituye un proceso de caracterización extraordinariamente útil para el análisis de las intrusiones. En el Modelo de Diamante se denomina **Proceso del Adversario** a aquel que resulta de agrupar Hilos de Actividad que compartan ciertas características comunes.
136. Por ejemplo, la figura siguiente muestra los Procesos del Adversario definidos a partir de los eventos 2, 3, 4 y 6 de la figura 7 anterior. El Hilo de Actividad así construido puede usarse para compararlo con otros Hilos de Actividad que pudieran mostrar el mismo orden en los eventos que lo componen y en sus características. Es importante señalar que el sub-grafo construido puede ser elástico, en el sentido de que cada caso particular analizado podría contener eventos adicionales incluidos en el Hilo de Actividad que se ha definido como patrón.


Fases del Ataque		Características del Proceso del Adversario
Reconocimiento		Búsqueda en la web de "administrador de red" [derivado del evento 2]
Código dañino		
Entrega		Entrega del correo electrónico con adjunto troyanizado [derivado del evento 3]
Explotación		Explotación de una vulnerabilidad específica (por ejemplo, CVE-YYYY-XXX) [derivado del evento 4]
Instalación		
C2		Post HTTP desde la víctima [derivado del evento 6]
Acción en el objetivo		

Figura 8: Ejemplo de Proceso del Adversario

3.6.2 SOPORTE AL ANÁLISIS DE HIPÓTESIS

137. Como se examina más adelante, el soporte a la generación de hipótesis, su documentación y ulterior prueba, constituye una de las características más importantes de los Hilos de Actividad, proporcionando una integración con otros modelos analíticos formales, tales como el mostrado en "The Analysis of Competing Hypotheses (ACH)"³³. En cualquier caso, 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.

³³ Richards J. Heuer Jr. Psychology of Intelligence Analysis. Central Intelligence Agency, 1999.

3.6.3 GRAFO DE ACTIVIDAD-ATAQUE

138. Los Hilos de Actividad del Modelo de Diamante y los clásicos *grafos de ataque* pueden, de manera combinada, dar respuesta a cuestiones complementarias. Así, los grafos de ataque identifican y enumeran los caminos que un adversario PODRÍA seguir, mientras que los Hilos de Actividad definen los caminos que el adversario HA seguido.
139. A la combinación de ambas representaciones es lo que, en labores de inteligencia, se ha denominado *Grafo de Actividad-Ataque*.
140. Los grafos de actividad-ataque proporcionan los siguientes beneficios:
- Manteniendo la integridad del grafo de ataque, hacen posible el análisis de su ámbito completo.
 - Incrementan la cantidad información que contiene un grafo de ataque, toda vez que cada nodo se configura como un Evento del Modelo de Diamante.
 - Incrementan la cantidad de información visual contenida en un grafo de ataque, sin reducir su usabilidad.
 - Generan apreciaciones cuantitativas más precisas.
 - Resaltan las preferencias del atacante a través de caminos alternativos.
 - Facilitan la comparación exhaustiva de caminos y escenarios alternativos y, en consecuencia, favorecen las campañas de mitigación.
 - Ayudan a rellenar las brechas de conocimiento de cualquier ataque usando patrones previamente conocidos.
141. La figura siguiente muestra un ejemplo de grafo de actividad-ataque. En ella se distinguen los caminos ya conocidos del adversario (Hilo de Actividad) y los posibles caminos que podrían ser explotados (grafo de ataque)³⁴.

³⁴ Esta representación es muy similar a las realizadas durante una prueba de penetración (Red Team) y su correspondiente evaluación de vulnerabilidades (Blue Team) para esbozar el mejor desarrollo de una acción concreta.

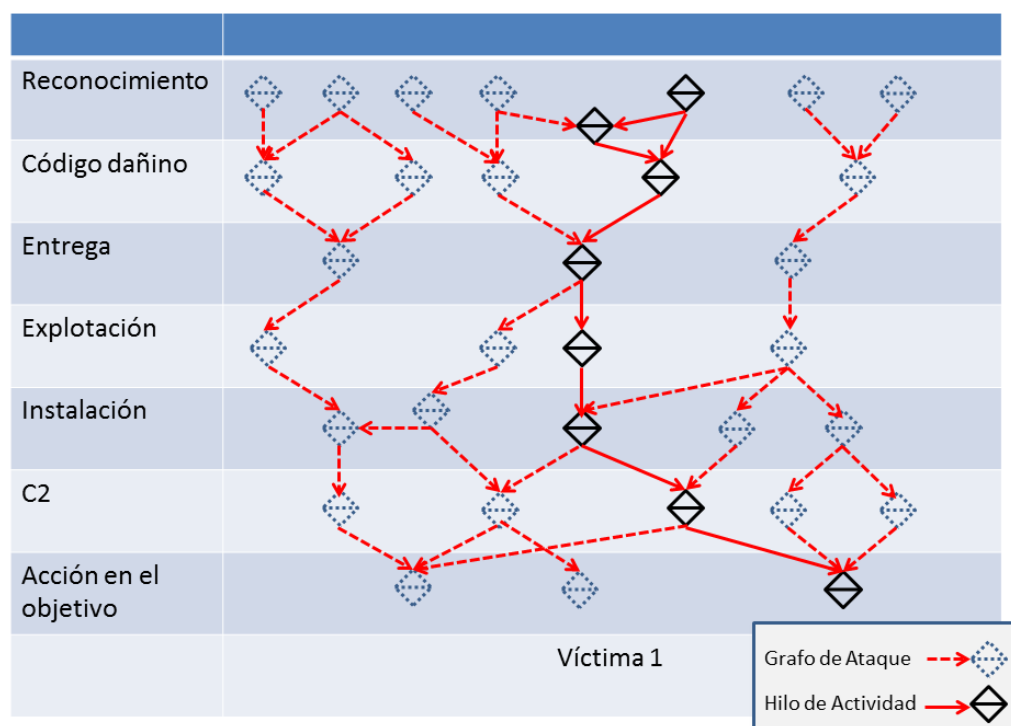


Figura 9: Ejemplo de Grafo de Actividad-Ataque

142. Como se ha dicho, los Hilos de Actividad y los grafos 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.

3.7. GRUPOS DE ACTIVIDAD

143. Un **Grupo de Actividad** es un conjunto de Eventos e Hilos de Actividad asociados por Características o Procesos del Adversario similares, y construido con un determinado grado de confianza.
144. Formalmente, podemos definir un Grupo de Actividad, **GA**, como un conjunto de Eventos e Hilos de Actividad que comparten una o más Características o Procesos del Adversario, de la forma:

$$GA = \{eh_1, eh_2, ..., eh_n\}$$

Dónde:

$n \geq 1$. Es decir, cada Grupo de Actividad debe contener, al menos, un elemento.

eh_n es un Evento singular o un Hilo de Actividad.

Todos los Eventos o Procesos del GA comparten una o más semejanzas que satisfacen la función de creación del Grupo de Actividad usada para dividir el conjunto total de Eventos e Hilos de Actividad.

145. La figura siguiente muestra un esquema conceptual de un Grupo de Actividad.

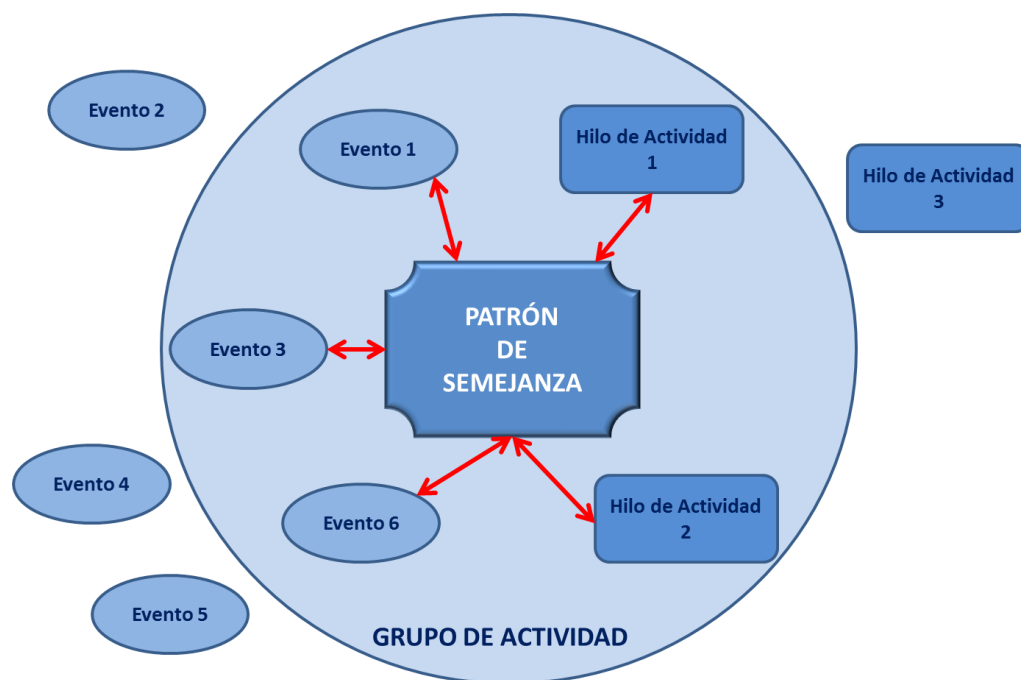


Figura 10: Grupo de Actividad

146. Un grupo de actividad tiene dos propósitos.
- (1) constituir un marco de trabajo para analizar y responder cuestiones que requieren de una amplia base de conocimiento y
 - (2) desarrollar estrategias de mitigación con resultados más amplios que los que puedan ofrecer los Hilos de Actividad.
147. Los Grupos de Actividad se diferencian de los Hilos de Actividad en dos cuestiones: 1. Los Grupos Actividad contienen tanto Eventos como Hilos, y 2. Los Eventos y los Hilos de un Grupo de Actividad se han construido en base a características y comportamientos concretos más que a relaciones de causalidad.
148. Pueden definirse los siguientes seis **pasos** en el proceso de análisis que involucra a los Grupos de Actividad:
- **Paso 1 - El problema a analizar:** que enuncia el problema o cuestión particular que debe ser analizada usando el agrupamiento de Eventos e Hilos.
 - **Paso 2 – Selección de Características:** que determina las Características y los Procesos del Adversario que se usarán como base para la clasificación (*clustering*) de todos ellos y la formación de grupos.
 - **Paso 3 – Creación:** que determina la creación de los grupos, partiendo de los Eventos e Hilos considerados.
 - **Paso 4 – Crecimiento:** que determina la posibilidad de incorporación de nuevos Eventos en los Grupos de Actividad ya constituidos.
 - **Paso 5 – Análisis:** donde se analizan los Grupos de Actividad en la dirección señalada por el enunciado del problema a analizar.

- **Paso 6 – Redefinición:** en el que los Grupos de Actividad se redefinen, al objeto de ajustar o mantener su fiabilidad.

149. Seguidamente, se desarrollan estos pasos.

3.7.1 PASO 1: EL PROBLEMA A ANALIZAR

150. Como se ha dicho, el agrupamiento de actividades se usa para resolver problemas que requieren mecanismos de deducción o de inferencia basados en un conjunto común de características. Este conjunto común de características es lo que se denomina **Vector de Características**.
151. Formalmente, puede definirse el problema a analizar, **PR**, como una pregunta de análisis de intrusiones que requiere de procedimientos de *clustering* y clasificación para su resolución, parcial o total.
152. Algunos ejemplos de problemas de esta naturaleza que pueden ser abordados a través de la creación de Grupos Actividad admiten las siguientes características:
- Tendencias: ¿Cómo se ha modificado en el tiempo la actividad de un adversario y qué puede inferirse de futuras modificaciones?
 - Deducción de intenciones: ¿Cuál es la intención última del adversario?
 - Deducción de la atribución: ¿Qué Eventos e Hilos de Actividad han sido probablemente desarrollados por el mismo adversario?
 - Capacidades e infraestructuras del adversario: ¿Cuál ha sido el conjunto completo de capacidades e infraestructuras usadas por el adversario?
 - Identificación de capacidades compartidas: ¿Qué capacidades han sido usadas por distintos adversarios?
 - Identificación de brechas en el conocimiento de las campañas del adversario: ¿Cuáles son las brechas de conocimiento que tiene la organización respecto de las campañas del adversario?
 - Recomendaciones de mitigación automática: Cuando se detecta que un adversario se halla detrás de un evento, ¿qué acciones pueden o deben seguirse?
 - Deducción de desarrollos o capacidades comunes: ¿Qué desarrollos o capacidades muestran evidencias de haber sido realizadas por los mismos autores?
 - Identificación del centro de gravedad: ¿Qué recursos y procesos han sido los más comunes o los más críticos para la víctima, de una actividad o una campaña del adversario?

3.7.2 PASO 2: SELECCIÓN DE CARACTERÍSTICAS

153. Los Eventos y los Hilos de Actividad se pueden agrupar de dos formas complementarias:
- (1) Usando varias características principales, meta-características o sub-características.
 - (2) Teniendo en cuenta Procesos del Adversario, previamente contemplados como sub-grafos de un Grupo de Actividad.
154. Para realizar la agrupación, y en base a un determinado criterio, se seleccionan determinadas características, constituyendo lo que se ha definido como **Vector de**

Características, que contendrá aquellos elementos que se usarán para agrupar Eventos e Hilos de Actividad³⁵.

155. Obviamente, el contenido de los Vectores de Características podrá ser tan general o tan específico como el analista considere necesario para facilitar el proceso de análisis.
156. Se denomina **Espacio de Características** el conjunto de todas las características-principales y meta-características de los eventos considerados. Partiendo de este Espacio de Características, las más importantes o significativas a efectos de análisis pasarán a formar parte del Vector de Características. Finalmente, a cada una de ellas podrá asignársele un determinado peso que denote su importancia relativa dentro del grupo al que pertenece.
157. La figura siguiente muestra un esquema gráfico de estos conceptos.

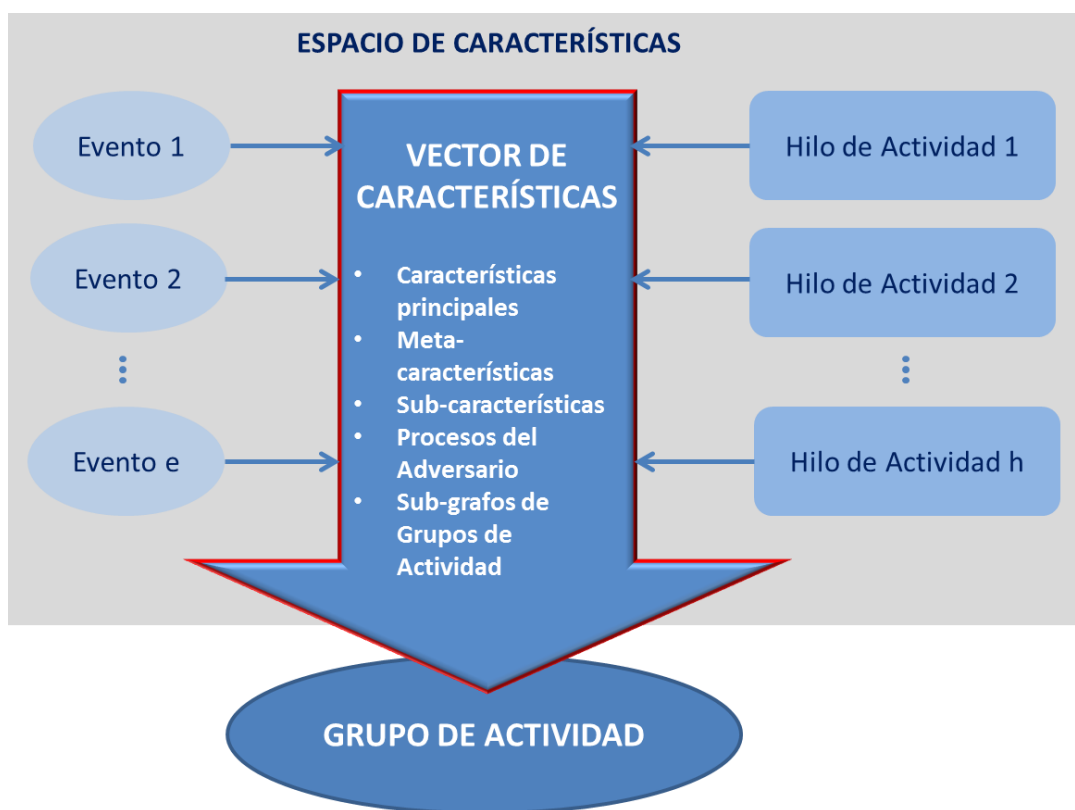


Figura 11: Formación de Grupos de Actividad en base al Vector de Características

158. El cuadro siguiente muestra un ejemplo de los Pasos 1 y 2 en la definición de un Grupo de Actividad.

El problema a analizar	¿Qué Eventos e Hilos de Actividad son los que con mayor probabilidad utiliza el Adversario en un cierto Proceso-1?
Espacio de Características	$Infraestructura_{IP}$, $Infraestructura_{Dominio}$, $Capacidad_{MD5}$, $Víctima_{IP}$

³⁵ Ver: Huan Liu and Hiroshi Motoda. Feature Selection for Knowledge Discovery and Data Mining. Kluwer Academic Publishers, Norwell, MA, USA, 1998.

	<i>Víctima</i> _{Organización} <i>Metodología</i> , <i>Proceso</i> ₁ , <i>Proceso</i> ₂ , <i>Proceso</i> ₃
Vector de Características	$\langle \text{Infraestructura}_{IP}, \text{Capacidad}_{MD5}, \text{Proceso}_1 \rangle$
Resultado	Formarán parte del mismo conjunto (Grupo de Actividad) todos los Eventos e Hilos de Actividad que compartan la Infraestructura IP, la Capacidad MD5 y se encuentren definidos dentro del Proceso-1 del adversario.

159. Formalmente, podemos definir el Espacio de Características, **EC**, como el conjunto de todas las características-principales, meta-características y sub-características definidas en todos los Eventos y Procesos del Adversario considerados.
160. Siguiendo con esta línea, podemos definir el Vector de Características para abordar un problema de análisis de intrusión, **VC_{PR}**, como:

$$VC_{PR} = \langle \langle c_1, p_{c1} \rangle, \langle c_2, p_{c2} \rangle, \dots, \langle c_n, p_{cn} \rangle \rangle$$

Dónde:

$n \geq 1$. Es decir, el vector de características debe tener, al menos, un elemento.

c_n pertenece a **EC**. Es decir, cada característica considerada en el Vector debe existir en Espacio de Características.

VC está contenido en el **EC**. Es decir, el Vector de Características es un subconjunto del Espacio de Características.

c_n es un elemento necesario para agrupar Eventos e Hilos, dirigido a resolver el problema de análisis planteado.

p_{cn} es un número real comprendido entre 0 y 1, y representa la importancia de dicha característica, siendo el valor 1 el que confiere la mayor importancia.

3.7.3 PASO 3: CREACIÓN

161. Básicamente, la creación de Grupos de Actividad se lleva a cabo a través de un proceso de *clustering* en el que el analista compara las características de un Evento con el patrón de semejanzas perseguido, obteniendo distintos grupos que comparten determinadas características. A estos grupos se les suele denominar **clases**, a partir de las cuales pueden utilizarse técnicas automáticas de detección y crecimiento.
162. La agrupación de Eventos e Hilos se deberá desarrollar siempre con el objetivo puesto en la resolución del problema de análisis que se hubiere definido. Obviamente, la organización podrá construir tantos Grupos de Actividad como problemas a analizar haya definido.
163. Formalmente, podemos definir la Función de Creación de Grupos de Actividad, **CGA**, como:

$$CGA (PR, VC_{PR}, EH) \rightarrow GAs$$

$$GAs = \{GA_1, GA_2, \dots, GA_n\}$$

Dónde:

PR es el problema de análisis que debe ser resuelto por la función de creación.

VC_{PR} es el Vector de Características que satisface el problema de análisis PR .

EH es el conjunto de todos los Eventos e Hilos de Actividad que deben ser agrupados.

CGA realizará una partición de todos los elementos (Eventos e Hilos) de EH en un conjunto de n Grupos de Actividad (GAs), tomando como base el Vector de Características del problema VC_{PR} .

La función CGA operará sobre todos los elementos del conjunto EH , usando las características y procesos definidos en VC_{PR} .

GAs es el conjunto de Grupos de Actividad, tales que cada Grupo de Actividad GA_n satisface la definición de Grupo de Actividad.

Es posible que la creación de la función de agrupamiento no produzca ningún grupo, si no existe ninguna semejanza entre los elementos analizados.

164. La figura siguiente muestra cómo puede definirse una función de creación de grupos de actividad (CGA) para resolver un problema concreto.

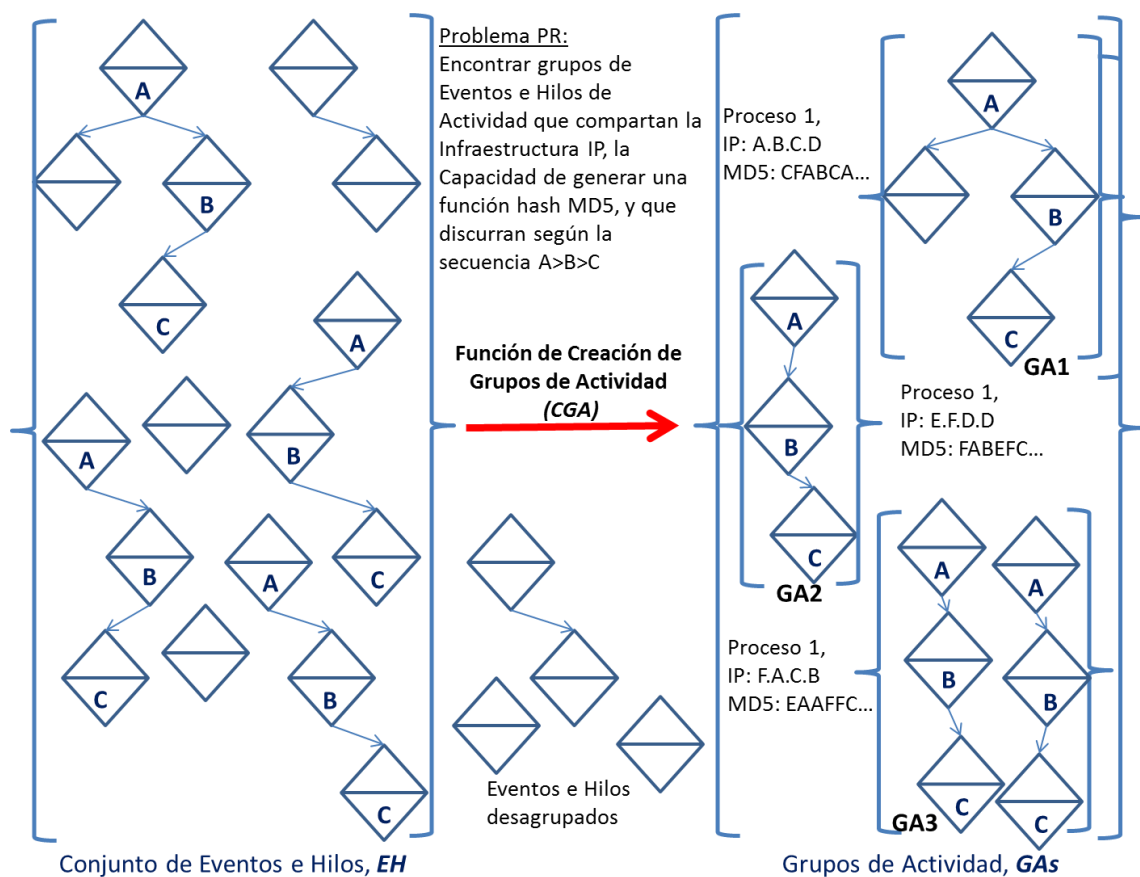


Figura 12: Creación de Grupos de Actividad

Como puede observarse en la figura anterior, a partir del conjunto total de Eventos e Hilos, *EH*, y de la función de creación, *CGA*, se han obtenido tres Grupos de Actividad, contruidos en base a las semejanzas que se han encontrado en función del Pproceso ($A \rightarrow B \rightarrow C$), de la Infraestructura IP utilizada y de su capacidad para generar hash MD5.

3.7.4 PASO 4: CRECIMIENTO

165. El proceso de análisis continuo de los diferentes comportamientos que los adversarios adoptan en el desarrollo de sus ataques facilita el crecimiento de los Grupos de Actividad, si en alguno de los nuevos ataques se observan semejanzas respecto de los Grupos que ya se hubieren constituido con anterioridad.
166. La figura siguiente muestra un ejemplo del crecimiento de los Grupos de Actividad creados en la Figura 12 anterior, partiendo de la detección de nuevos Eventos e Hilos de Actividad.

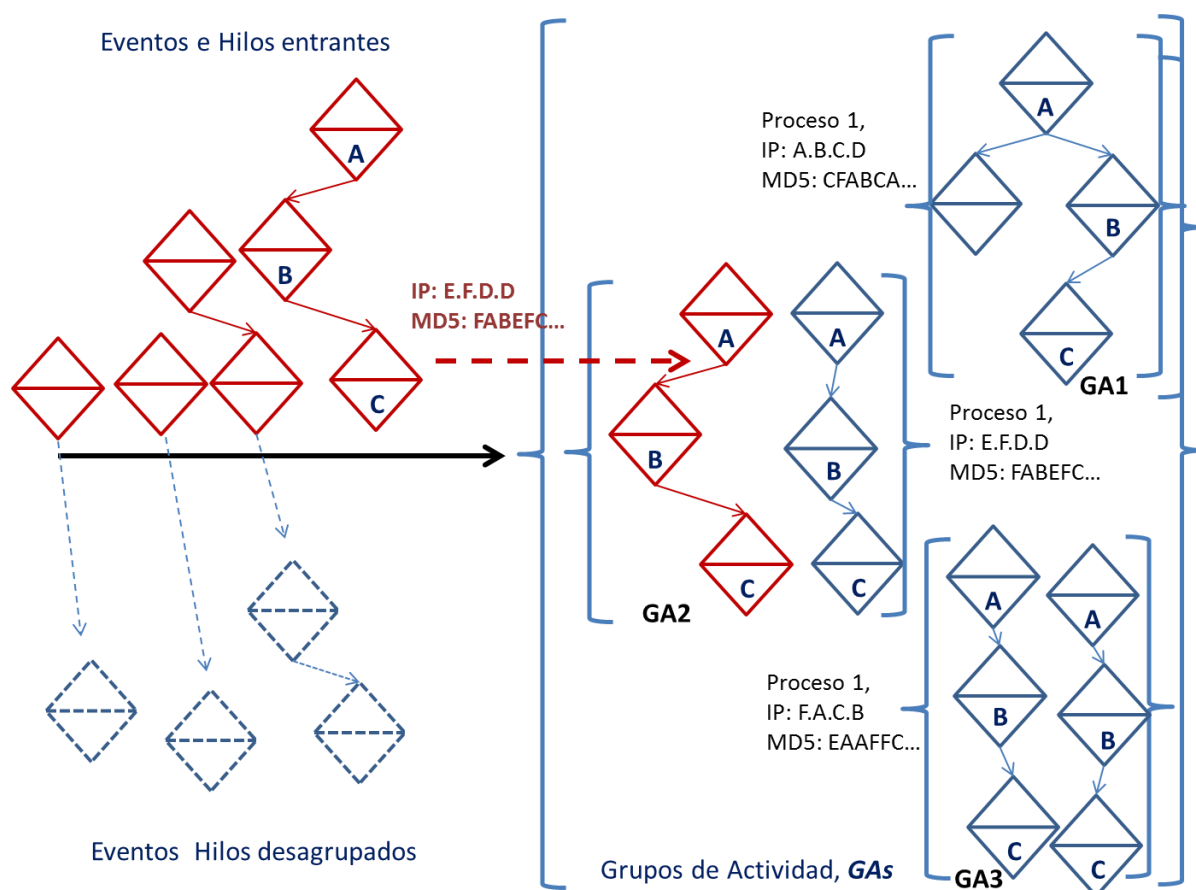


Figura 13: Crecimiento de los Grupos de Actividad

3.7.5 PASO 5: ANÁLISIS

167. Una vez que se han obtenido los Grupos de Actividad, agrupando Eventos e Hilos de Actividad, ya es posible realizar el análisis correspondiente en base al problema planteado.
168. Esta actividad de análisis puede realizarse de manera exclusivamente manual o contando con la ayuda de herramientas automatizadas.

169. Sea como fuere, si los pasos anteriores se han desarrollado adecuadamente, el analista dispone en este momento de la información que precisa para analizar con exhaustividad los Eventos de intrusión y los Hilos de Actividad del adversario, incluyendo: campañas del adversario a largo plazo, identificación entre eventos similares o diferentes, recopilación y documentación de las capacidades e infraestructuras usadas por el adversario, elementos para la reducción de la autoría de los ataques, etc.
170. Como veremos, es posible que, durante el análisis, sea necesario redefinir los elementos que conforman el Vector de Características.

3.7.6 PASO 6: REDEFINICIÓN

171. Como se ha afirmado, la función de creación de los Grupos de Actividad, como sucede con todas las funciones de *clustering*, puede presentar ciertos riesgos bien definidos. Uno de tales inconvenientes es asumir indubitadamente que el analista siempre está en condiciones de describir con precisión el Vector de Características usado para agrupar los Eventos e Hilos de Actividad. Otro de los retos es el derivado del necesario ajuste de las características para evitar el error de propagación, en el que un analista (o un sistema automatizado) podría asociar de manera equivocada un Evento a un determinado Grupo, propagando y magnificando el error.
172. Por todo ello, es normal que la función de creación de los Grupos de Actividad precise de un examen constante, capaz de detectar anomalías que hagan necesaria una redefinición (*reclustering*) que corrija los errores detectados. Durante esta etapa de redefinición, los ajustes pueden (y suelen) afectar al Vector de Características, a los pesos otorgados y a los algoritmos usados.

3.7.7 FAMILIAS DE GRUPOS DE ACTIVIDAD

173. Como hemos señalado, los Grupos de Actividad pueden ser tan variados como las organizaciones que se encuentran detrás de la actividad dañina. Por este motivo, puede ser necesario en ocasiones desarrollar una jerarquía de grupos mediante la cual modelar la compleja organización que se esconde detrás de los eventos, y todo ello de cara a dar respuesta a preguntas de mayor calado o desarrollar mejores estrategias de mitigación.
174. Podemos definir una **Familia de Grupos de Actividad** como conjunto de Grupos Actividad que comparten características comunes, sin contar con que, muchas veces, las características comunes de tales grupos pueden ser de naturaleza no-técnica (financiación común, por ejemplo, etc.)
175. Para los propósitos de la metodología de análisis que se propone, las Familias de Grupos de Actividad serán tratadas con los mismos seis pasos descritos con anterioridad. Tales familias tendrán, por consiguiente, sus Vectores de Características y sus propias Funciones de Creación.
176. Formalmente, podemos definir una familia de grupos de actividad como:

$$FGA = \{GA_1, GA_2, \dots, GA_n\}$$

Dónde:

$n \geq 1$. Es decir, una Familia de Grupos de Actividad debe contener, al menos, un Grupo de Actividad.

GA_n satisface la definición de Grupo de Actividad.

FGA es un conjunto de Grupos de Actividad que comparten una o más semejanzas.

FGA satisface un problema de análisis concreto.

FGA es el resultado de una Función de Creación y un Vector de Características que compara Grupos de Actividad.

3.8. PLANIFICACIÓN

177. El Modelo de Diamante proporciona un buen conocimiento de las dependencias que existen entre los componentes del adversario. Para que los esfuerzos del adversario se vean coronados con el éxito, debe construir un camino entre la intención y el resultado. El Modelo de Diamante ayuda a comprender cómo las acciones de defensa podrían impactar en las capacidades del adversario, determinando los componentes que deberá establecer, reemplazar o reelaborar el atacante.
178. El modelo ayuda a estructurar y fortalecer el análisis de intrusiones para alcanzar su último objetivo: la mitigación. Los párrafos siguientes muestran la aplicabilidad del modelo cuando se usan algunos sistemas de planificación y decisión muy conocidos.
179. **(1) Joint Intelligence Preparation of the Operational Environment (JIOPE):** JIOPE³⁶ es un recurso muy conocido, que establece un procedimiento para usar la inteligencia para desarrollar “cadenas de acción”. Esta aproximación identifica áreas óptimas de mitigación y contrarresta las capacidades del adversario para mantener y reconstruir aquellas capacidades e infraestructuras una vez que han sido inutilizadas o desmanteladas.
180. El Modelo de Diamante soporta JIOPE del siguiente modo:
 - Ayuda en la identificación de las brechas de inteligencia e información, mediante la determinación de características desconocidas de los Eventos y el descubrimiento de las lagunas de conocimiento que pudieran contener las fases de los Hilos de Actividad (JIOPE Step 1, Element 6).
 - Soporta el desarrollo de un modelo de adversario (JIOPE Step 3, Element 1).
 - Identifica la Infraestructura y Capacidades del adversario poniendo el foco en los Recursos (JIOPE Step 3, Element 3).
 - Identifica los centros de gravedad del adversario a través de los Hilos de Actividad y el análisis de Grupos de Actividad (JIOPE Step 3, Element 4).
 - Identifica los objetivos del adversario a través del análisis de los Hilos de Actividad, victimología y Grupos de Actividad (JIOPE Step 4, Element 1).
 - Determina la probabilidad de ocurrencia de las cadenas de acción del adversario, a través del análisis de Grafos de Actividad-Ataque, identificando sus potenciales o preferidos caminos de ataque (JIOPE Step 4, Elements 2 and 3).
181. **(2) Análisis Kill Chain:** El denominado Modelo Kill Chain³⁷ fue desarrollado para abordar, esencialmente, el análisis de APTs³⁸ (Amenazas Persistentes Avanzadas), toda vez que permite describir las diferentes fases que componen una intrusión, comparando distintos indicadores de las “fases de ataque” (*kill chain*) usadas por el adversario, para identificar patrones de intrusión que permitan enlazar acciones individuales con campañas

³⁶ US Department of Defense. Joint Tactics, Techniques, and Procedures for Joint Intelligence Preparation of the Operational Environment (JP 2-01.3), June 2009.

³⁷ Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. Eric M. Hutchins, Michael J. Clopperty, Rohan M. Amin, Ph.D.z. Lockheed Martin Corporation

³⁸ Advanced Persistent Threats

de mayor extensión, haciendo uso de la naturaleza cíclica de la recopilación de inteligencia, sobre la base de una Defensa de Redes de Ordenadores (*Computer Network Defence* – CND) dirigida por la inteligencia. Como se ha demostrado, la implantación de este tipo de análisis reduce la probabilidad de éxito del adversario, señala prioridades en la asignación de recursos, proporcionando al tiempo métricas para la determinación de la eficiencia alcanzada. La evolución de las APTs exige disponer de un modelo de análisis dirigido por la inteligencia capaz no sólo de mitigar las vulnerabilidades de los sistemas, sino también los componentes de riesgo de la propia amenaza.

182. Esencialmente, una **Defensa de Redes de Ordenadores (CND) dirigida por la inteligencia** es una estrategia de gestión de riesgos que se centra en los componentes del riesgo, a través del análisis de los adversarios, sus capacidades, objetivos, doctrina y limitaciones. El elemento fundamental de la inteligencia en este modelo es el **indicador**, que consiste en una pieza de información que, de forma objetiva, describe una intrusión, subdividiéndose en: **indicadores atómicos** (aquellos que no pueden ser divididos en unidades más pequeñas, permaneciendo invariables durante el transcurso de una intrusión, tales como direcciones IP, direcciones de correo electrónico e identificadores de vulnerabilidades, por ejemplo); **indicadores calculados** (aquellos que se derivan de los datos de un incidente, tales como valores hash y expresiones regulares, por ejemplo); y **indicadores de comportamiento** (formados por colecciones de indicadores atómicos para los que puede encontrarse una relación causal).
183. De forma análoga a lo que sucede con el Modelo de Diamante, Kill Chain divide la acción del adversario en **fases**: Reconocimiento, Código Dañino, Entrega, Explotación, Instalación, Mando y Control (C2) y Acción en el Objetivo, constituyendo un modelo para la obtención de inteligencia acabada, toda vez que posibilita el alineamiento de las capacidades defensivas de la organización víctima con los procesos de ataque que el adversario podría utilizar contra tal organización. El modelo permite a la víctima medir la eficiencia de las medidas adoptadas, sirviendo de ayuda para planificar una hoja de ruta de las acciones e inversiones precisas para resolver las brechas encontradas.
184. En resumen: mientras que el análisis Kill Chain permite a un analista “dirigir la actividad del adversario para lograr los objetivos deseados”, el Modelo de Diamante permite a los analistas desarrollar mecanismos para construir y organizar el conocimiento necesario capaz de ejecutar el análisis Kill Chain anterior.
185. Ambos métodos pueden integrarse de las siguientes dos maneras:
 - Una vez que el analista ha desarrollado un Hilo de Actividad, las líneas de acción de cada Evento o a lo largo del Hilo puede identificarse usando una matriz Kill Chain. La figura siguiente muestra las *líneas de acción (courses of action)* que resultan de cada fase identificada en nuestro ejemplo de la Figura 7.

Fases del ataque	Líneas de acción					
	Detección	Denegación	Disrupción	Degradación	Engaño	Destrucción
Reconocimiento	Análisis Web	Política para prevenir uso en foros			Crear posts simulados	
Código dañino						
Entrega	NIDS ³⁹ formación del usuario	Exploración del correo		Encolado del correo	Filtrado, respondiendo con un mensaje de "fuera de la oficina"	
Explotación	HIDS ⁴⁰	Parche	DEP ⁴¹			
Instalación						
C2	NIDS	HTTP Whitelist	NIPS	HTTP ⁴² Colapso		
Acción en el objetivo	Detección Proxy	Firewall ACL ⁴³	NIPS	HTTP Colapso	Honeypot ⁴⁴	

En la matriz anterior, puede observarse que, para cada una de las fases que constituyen el ataque, el modelo Kill Chain contempla seis posibles *líneas de acción* (Detección, Denegación, Disrupción, Degradación, Engaño y Destrucción) que la víctima puede utilizar para situar mecanismos o herramientas que sirvan para mitigar los riesgos que aparecen en cada una de ellas.

- Los Grupos de Actividad, contruidos en base al mismo adversario probable (*clustering* por atribución), con el análisis del conjunto de características comunes entre los eventos de un Grupo, pueden proporcionar los indicadores de campaña requeridos por Kill Chain y necesarios para focalizar y priorizar las cadenas de acción.

186. **(3) Protección de las vulnerabilidades:**

187. Una práctica común en el aseguramiento de la información es analizar un sistema (o una red) en búsqueda de vulnerabilidades, priorizando aquellas que pudieran afectar a activos esenciales para la organización. Tras este análisis se aplican las medidas de mitigación para las vulnerabilidades seleccionadas.
188. A través de la generación de Grafos de Actividad-Ataque, este proceso de selección de vulnerabilidades (que suele comportar un riesgo evidente) puede desarrollarse a través de las preferencias del adversario y de sus potenciales capacidades.

³⁹ Network Intrusion Detection System,

⁴⁰ Host Intrusion Detection System.

⁴¹ Data Execution Prevention

⁴² Hyper Text Transfer Protocol.

⁴³ Access Control List.

⁴⁴ Sistema trampa diseñado para engañar a posibles intrusos.

3.9. CONCLUSIONES DEL MODELO.

189. Los epígrafes anteriores han mostrado el Modelo de Diamante para el análisis de intrusiones, que arranca con la definición de lo que constituye su elemento esencial: el Evento, y las Características (principales, meta y sub) que lo definen.
190. Partiendo del Evento se han desarrollado aproximaciones con origen en sus distintas características, sirviendo de ayuda a la categorización de los procesos de análisis y, al mismo tiempo, al descubrimiento de nuevos procesos.
191. El Modelo de Diamante captura la esencia de la actividad de intrusión como un conjunto de eventos causales involucrados en el denominado Hilo de Actividad, que describe el Proceso (de ataque) de un Adversario. La descripción de estos Hilos de Actividad se amplía con los que denominamos Grafos de Ataque, de cara a crear una nueva aproximación centrada en la inteligencia a la que denominamos Grafos de Actividad-Ataque, tomando en consideración no sólo los ataques reales sino también los potenciales o los caminos preferidos por el adversario. Buscando la semejanza entre Hilos de Actividad y Eventos se desarrolló el concepto de Grupos de Actividad, cuyo objetivo se dirige a la realización de un análisis más amplio de los eventos de intrusión, de cara a desarrollar campañas de mitigación más eficaces.
192. Por último, los Grupos de Actividad se organizaron jerárquicamente en Familias, concentración que puede utilizarse para modelar más eficazmente a las organizaciones adversarias de naturaleza más compleja.

ANEXO 1. REFERENCIAS

Además de las señaladas en los pies de página que se han incluido a lo largo del texto, señalamos las siguientes:

- Guía CCN-STIC 403 Gestión Incidentes de Seguridad.
- Guía CCN-STIC 423 Indicadores de compromiso (IOC).
- Guía CCN-STIC 424 Intercambio de información de ciberamenazas. STIX-TAXII. Empleo en REYES (en preparación).
- Guía CCN-STIC 431 Herramientas de Análisis de Vulnerabilidades.
- Guía CCN-STIC 426 REYES: Manual de Usuario (en preparación).
- Guía CCN-STIC 817 Gestión de Ciberincidentes (ENS).
- Guía CCN-STIC 911A Ciclo de una APT (Difusión Limitada)