



Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

Operaciones Cyber ISR (CISRO)

Máster Universitario en Dirección TIC para la Defensa

ALUMNO: Carlos Díez Gago

DIRECTORES: Miguel Rodelgo Lacruz

CURSO ACADÉMICO: 2025-2026

Universida_{de}Vigo

PÁGINA INTENCIONADAMENTE EN BLANCO



Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

Operaciones Cyber ISR (CISRO)

Máster Universitario en Dirección TIC para la Defensa
Especialidad de Sistemas y Tecnologías de Telecomunicación

UniversidadeVigo

PÁGINA INTENCIONADAMENTE EN BLANCO

RESUMEN

Al igual que en el resto de los dominios tradicionales del campo de batalla (terrestre, marítimo, aéreo, y espacial), en el dominio del ciberespacio también se llevan a cabo operaciones ISR, en este caso adaptadas y orientadas a las vicisitudes técnicas del dominio. Este tipo de operaciones proporcionan la inteligencia necesaria para conocer al enemigo, sus tácticas técnicas y procedimientos (TTP) y las vulnerabilidades propias y ajenas para anticiparse a futuros ataques o incluso proporcionar puntos de entrada para realizar operaciones ofensivas.

Este trabajo de fin de Máster se enfoca en las tres capacidades que componen las operaciones ISR, que son la Inteligencia (Intelligence), Vigilancia o Cibervigilancia (Surveillance) y el Reconocimiento (Reconnaissance).

El trabajo comienza con una revisión doctrinal del dominio ciberespacial, así como de los tipos de operaciones que se conducen en él, para posteriormente pasar a analizar con más detalle las operaciones CISRO atendiendo a las capacidades antes mencionadas y ofrecer una metodología de planeamiento y ejecución de este tipo de operaciones.

Del análisis de la información recopilada se deduce que la Inteligencia de Ciberamenazas (CTI) tiene cabida en el enfoque doctrinal del ciclo de la inteligencia clásica, que la Cibervigilancia se constituye como un elemento de alerta temprana ante futuros ataques y que el Reconocimiento posibilita el conocimiento de las vulnerabilidades y la superficie de ataque propia y del enemigo.

Finalmente se llega a que las tres capacidades estudiadas (Inteligencia, Cibervigilancia y Reconocimiento) no deben considerarse como compartimentos estancos, sino como fases complementarias de un mismo proceso orientado a garantizar la superioridad de la información en el campo de batalla.

PALABRAS CLAVE

Ciberespacio, inteligencia, cibervigilancia, reconocimiento, TTP.

PÁGINA INTENCIONADAMENTE EN BLANCO

AGRADECIMIENTOS

A mi mujer Susana y mi hijo Carlos, por aceptar con agrado mi situación como estudiante y apoyarme en esta navegación, sobre todo en las singladuras presenciales de Marín que implicaron mi ausencia.

A mi tutor, Miguel, por su inestimable ayuda, guía y predisposición. Su experiencia me ha servido de guía para enfrentarme a este trabajo académico y poderlo llevar a buen puerto.

A los profesores del Centro Universitario de la Defensa (CUD) de la Universidad de Vigo que han impartido cada una de las asignaturas del Máster, así como al personal de la Escuela Naval Militar, que me ha posibilitado volver a la casa madre y me ha proporcionado el apoyo logístico necesario en las fases presenciales del Máster en Marín.

Al Mando Conjunto del Ciberespacio (MCCE) y mis compañeros anónimos, ellos saben quiénes son. Sin ellos no habría adquirido ni la experiencia ni los conocimientos que hoy tengo en esta materia.

A mis compañeros de la Jefatura de Sistemas de Información y Telecomunicaciones (JECIS), del Estado Mayor de la Armada y de la Dirección de Enseñanza Naval (DIENA) por las facilidades que me han ofrecido en el desarrollo de las prácticas de la Especialidad de Segundo Tramo de la Armada (E2T TCI-Ciber), de la que es parte este Máster.

A mis compañeros del Máster, un grupo excepcional en lo profesional y en lo personal. Además del conocimiento adquirido, me llevo amigos.

PÁGINA INTENCIONADAMENTE EN BLANCO

CONTENIDO

Contenido	1
Índice de Figuras	5
Índice de Tablas.....	9
1 Introducción y objetivos	11
1.1 Contexto General	11
1.2 Problema y relevancia del estudio	12
1.3 Objetivos	12
1.4 Metodología	13
1.5 Estructura	13
2 Estado del arte	15
2.1 Ciberespacio.....	15
2.2 Estructura y organización de un Mando militar ciber.....	16
2.2.1 Security Operations Centre (SOC)	17
2.2.2 Computer Emergency Team (CERT)	18
2.2.3 Rapid Reaction Team (RRT)	18
2.2.4 Elementos de enlace	18
2.3 Tipos de ciberoperaciones.....	18
2.3.1 CISIO.....	19
2.3.2 DCO	19
2.3.3 OCO	20
2.3.4 CISRO.....	20
2.4 Efectos.....	21
2.5 Consideraciones legales en las operaciones CISRO	22
3 Inteligencia	25
3.1 Fase de Dirección.....	27
3.1.1 Modelado de amenazas	27
3.1.2 Necesidades de información	28
3.1.3 Plan de obtención.....	30
3.2 Fase de Obtención.....	32
3.2.1 Tipología de fuentes para CTI	32
3.2.2 Indicadores de compromiso	32
3.2.3 Pirámide del dolor.....	33
3.3 Fase de Elaboración	34
3.3.1 Identificación de TTP mediante MITRE ATT&CK.....	34

3.3.2 Cyber Kill Chain.....	35
3.3.3 Diamond Model.....	38
3.3.4 Correlación de eventos	38
3.3.5 Identificación de campañas.....	39
3.3.6 Atribución.....	40
3.3.7 Mitigación. Matriz de cursos de acción.	43
3.4 Fase de Difusión.....	44
3.4.1 Sensibilidad de la información	45
3.4.2 Estándares de compartición	46
3.4.3 Plataformas de compartición	47
4 Cibervigilancia	51
4.1 Monitorización de dominios fraudulentos	51
4.2 Monitorización de fugas de información	53
4.3 Hacktivismo	54
4.3.1 Grupos más destacados.....	55
4.3.2 Ataques más comunes.....	57
4.3.3 Monitorización del hacktivismo	57
4.4 Monitorización de reputación	58
4.5 Disciplinas de obtención para cibervigilancia	58
4.5.1 Inteligencia de Fuentes Abiertas (OSINT)	58
4.5.2 Inteligencia en redes sociales (SOCMINT).....	59
4.5.3 Virtual HUMINT (VHUMINT)	64
4.6 Redes a monitorizar	65
4.6.1 Surface Web.....	66
4.6.2 Deep Web	66
4.6.3 Dark Web.....	66
5 Reconocimiento.....	69
5.1 Reconocimiento pasivo de infraestructura.....	69
5.1.1 Búsqueda de dominios del objetivo	69
5.1.2 Enumeración de DNS	70
5.1.3 Enumeración de subdominios.....	73
5.1.4 Resolución inversa de DNS	74
5.1.5 Búsqueda de host virtuales	75
5.2 Reconocimiento activo de infraestructura.....	75
5.2.1 Identificación de host activos	75
5.2.2 Escaneo de puertos	76

5.2.3 Analizadores de vulnerabilidades	79
5.2.4 Fuzzing de aplicaciones WEB	79
5.2.5 Análisis de las vulnerabilidades encontradas	81
5.3 Reconocimiento de infraestructura inalámbrica	84
5.3.1 Wardriving	84
5.3.2 Enumeración pasiva	84
5.3.3 Enumeración activa	85
5.4 Reconocimiento de las personas	86
5.5 Superficie de exposición	87
5.6 Vectores de ataque	88
5.7 Enumeración interna	91
6 Conclusiones y líneas futuras	94
6.1 Conclusiones	94
6.2 Líneas futuras	95
7 Bibliografía.....	96

PÁGINA INTENCIONADAMENTE EN BLANCO

ÍNDICE DE FIGURAS

Figura 2-1 Capas que comprenden el ciberespacio (acqnotes, s.f)	15
Figura 2-2 Ciberamenazas y acciones que utilizan el ciberespacio con fines maliciosos (DSN, 2019)	16
Figura 2-3 Organización tipo de un Mando Ciber (CCDCOE, 2020).....	17
Figura 2-4 Funciones de un SOC (Comodo, s.f.).....	17
Figura 2-5 Funciones de un CERT (GeeksforGeeks, 2024).....	18
Figura 2-6 Framework de operaciones en el ciberespacio (CCDCOE, 2020)	21
Figura 2-7 Manual de Tallin 2.0 (Securityaffairs, 2017).....	22
Figura 3-1 Relación entre datos, información e inteligencia (Huarui, 2022).....	25
Figura 3-2 Tipos de inteligencia de ciberamenazas según la audiencia objetivo (Guerra, 2023)	26
Figura 3-3 Fases del ciclo de inteligencia (EMAD, 2020).....	26
Figura 3-4 Inventariado y valoración de los activos de una organización (elaboración propia).....	27
Figura 3-5 Modelado de la amenaza a nivel estratégico (elaboración propia).....	28
Figura 3-6 Análisis de riesgos de una organización (elaboración propia)	28
Figura 3-7 Ejemplo del feed de CTI Alien Vault OTX (Zafra, 2025)	32
Figura 3-8 Ciclo de vida de un IoC (SANS Institute, 2009)	33
Figura 3-9 Pirámide del dolor (Bianco, 2025)	34
Figura 3-10 Mapeo de TTP de un atacante según Mitre ATT&CK (MB Secure, 2019)	35
Figura 3-11 Cyber Kill Chain de Lockheed Martin (Lockheed Martin, s.f.)	36
Figura 3-12 Ejemplo de aplicación del modelo del diamante (elaboración propia).....	38
Figura 3-13 Grupo de actividad (CCN, 2015).....	39
Figura 3-14 Triada del ataque (Dean, 2024)	41
Figura 3-15 Ejemplo de documento con cabecera TLP:GREEN (Altvater, s.f.)	46
Figura 3-16 Ejemplo de reporte STIX 2.1 (elaboración propia)	47
Figura 3-17 Modos de operación de TAXII (Davidson et al., 2017)	47
Figura 3-18 Vista de eventos en MISP (Bernabé et al., 2020).....	48
Figura 3-19 Dashboard de la herramienta The Hive (IristT, 2024).....	48
Figura 3-20 Dashboard de la herramienta OpenCTI (Frayssinet, 2024)	49
Figura 4-1 Dominios maliciosos asociados a la empresa CrowdStrike (Akamai, 2024).....	52
Figura 4-2 Correo malicioso con técnica de homoglifos (elaboración propia).....	52
Figura 4-3 Mayores brechas de datos de 2024 clasificadas por tipo (McCandless et al., 2024).....	54
Figura 4-4 Publicación en foro de información robada (Abrams, 2020)	54
Figura 4-5 Logotipo del grupo hacktivista Anonymous (Bertriu, 2013)	55
Figura 4-6 Reivindicación de ciberataque contra la web de la CIA por LulzSec (Benedetti, 2011).....	55

Figura 4-7 Ejemplo de ataque de NoName057(16) contra España (Piña, 2025)	56
Figura 4-8 Características del grupo hacktivista Cyber Army of Russia Reborn (SOCRadar, 2024)	56
Figura 4-9 Anuncio de ataques de High Society contra el sector energético de EEUU (Jain, 2024)	57
Figura 4-10 Monitorización del canal de Telegram de Noname057(16) (TGStat, s.f.)	57
Figura 4-11 Proceso OSINT (Martínez, 2014)	59
Figura 4-12 Aplicaciones estratégicas de SOCMINT (Goberna, 2025)	60
Figura 4-13 Mapeo de localización de seguidores (Lincoln, 2015)	61
Figura 4-14 Ejemplo de herramienta de investigación de Facebook (CCAS, 2020)	61
Figura 4-15 Vista de herramienta de OSINT en Instagram (San José, 2022b)	62
Figura 4-16 Ejemplo de herramienta de geolocalización en Telegram (Esgeeks, s.f.)	63
Figura 4-17 Comparativa de cuenta real y falsa en X de Cristiano Ronaldo (OKDiario, 2015)	64
Figura 4-18 Capas que componen Internet (Fernández, 2024)	66
Figura 4-19 Cifrado onion de red Tor con 3 nodos (Carles, 2016)	67
Figura 4-20 Túneles y nodos I2P (Rodríguez, 2017)	67
Figura 5-1 Consulta WHOIS de uvigo.gal (elaboración propia)	70
Figura 5-2 Fragmento de información obtenida por RDAP de uvigo.gal (elaboración propia)	70
Figura 5-3 Registros DNS de uvigo.gal (elaboración propia)	73
Figura 5-4 Ejemplo de resolución inversa por DNS (elaboración propia)	74
Figura 5-5 Ejemplo de Ping Sweep (elaboración propia)	76
Figura 5-6 TCP 3-way handshake (Goedebure, 2018)	77
Figura 5-7 Puerto TCP abierto (Goedebure, 2018)	77
Figura 5-8 Puerto TCP cerrado (Goedebure, 2018)	77
Figura 5-9 Puerto TCP filtrado (Goedebure, 2018)	77
Figura 5-10 Respuestas UDP en escaneo (Geeksforgeeks, 2025)	78
Figura 5-11 Ejemplo de escaneo de servicios y versiones con NMAP (elaboración propia)	78
Figura 5-12 Ejemplo de obtención de Sistema Operativo con NMAP (elaboración propia)	79
Figura 5-13 Escáner de vulnerabilidades Nessus (Bugcrowd, s.f.)	79
Figura 5-14 Ejemplo de Fuzzing de inyección SQL (Pointing, s.f.)	81
Figura 5-15 CVE mostrados en base de datos de NVD (NIST, s.f.)	82
Figura 5-16 Cuantificación de la severidad según NVD (NIST, s.f.)	82
Figura 5-17 Conjuntos de métricas que componen CVSSv4 (FIRST, s.f.a)	83
Figura 5-18 Muestra de la calculadora de CVSSv4 (NIST, s.f.)	83
Figura 5-19 Redes Wi-Fi reportadas en el Aeropuerto de Vigo (elaboración propia)	85
Figura 5-20 Ejemplo de enumeración activa de redes Wi-Fi (Promwad, s.f.)	86
Figura 5-21 Ejemplo de superficie de exposición de una organización (elaboración propia)	87

Figura 5-22 Vista del cuadro de mandos de la herramienta ELSA (CCN-CERT, s.f.).....	88
Figura 5-23 Selección de vectores de ataque (Lee, 2025).....	88
Figura 5-24 Ejemplo de enumeración automática con herramienta BloodHound (SANS Institute, 2021)	92

PÁGINA INTENCIONADAMENTE EN BLANCO

ÍNDICE DE TABLAS

Tabla 3-1 Necesidades de información a nivel estratégico (elaboración propia).....	29
Tabla 3-2 Necesidades de información a nivel operacional (elaboración propia)	29
Tabla 3-3 Necesidades de información a nivel táctico (elaboración propia)	30
Tabla 3-4 CMF para superficie de exposición (elaboración propia).....	31
Tabla 3-5 CMF de obtención de información interna para un SOC (Goss, 2024).....	31
Tabla 3-6 Perfilado de un ataque combinando Kill Chain y Mitre ATT&CK (elaboración propia).....	37
Tabla 3-7 Evaluación de hipótesis con método ACH (elaboración propia).....	40
Tabla 3-8 Ejemplo de Matriz ACH para atribución (elaboración propia).....	42
Tabla 3-9 Ejemplo de matriz de cursos de acción (Amin et al., s.f.)	44
Tabla 3-10 Grados de clasificación de seguridad (CCN, 2012; Hyden, 2025)	45
Tabla 4-1 Ejemplos de homoglifos (elaboración propia).....	52
Tabla 4-2 Ejemplos de combosquatting (elaboración propia).....	53
Tabla 4-3 Ejemplos de tiposquatting (elaboración propia)	53
Tabla 4-4 Ejemplos de TLD squatting (elaboración propia).....	53
Tabla 4-5 Aportación extra de VHUMINT respecto a OSINT y SOCMINT (DeBolt, 2023).....	65
Tabla 5-1 Tipos de registros DNS (Kurose & Ross, 2010).....	72
Tabla 5-2 Enumeración de subdominios de uvigo.gal (elaboración propia).....	74
Tabla 5-3 Ejemplo de Host virtuales (elaboración propia)	75
Tabla 5-4 Códigos HTTP útiles para fuzzing (Pointing, s.f.).....	80
Tabla 5-5 Ejemplos de vectores de ataque (LetsDefend, 2023).....	90
Tabla 5-6 Ejemplo de vulnerabilidad y vectores de ataque orientados a un Blue Team (elaboración propia)	90
Tabla 5-7 Ejemplo de vectores de ataque orientados a un Red Team (elaboración propia)	91

PÁGINA INTENCIONADAMENTE EN BLANCO

1 INTRODUCCIÓN Y OBJETIVOS

1.1 Contexto General

Las tecnologías de la información y la comunicación (TIC) han propiciado una transformación digital en todos los sectores, conllevando con ello un aumento en la superficie de exposición a amenazas y por ello la aparición de actores maliciosos que aprovechan las vulnerabilidades que éstas ofrecen. En los últimos años organismos internacionales como la OTAN y la Agencia de la Unión Europea para la Ciberseguridad (ENISA) han observado y advertido del repunte de las amenazas en el ciberespacio, siendo éstas cada vez más complejas y destructivas (ENISA, 2024; NATO, 2024a).

En este marco, los Estados y organizaciones internacionales han reconocido la necesidad de conceptualizar el ciberespacio como un dominio de operaciones, al mismo nivel que tierra, mar, aire y espacio. España, alineada con este enfoque, también ha incorporado el ciberespacio como un eje esencial en su Estrategia Nacional de Ciberseguridad, subrayando la importancia de proteger tanto sus infraestructuras críticas como sus intereses estratégicos (DSN, 2019).

En la cumbre de Varsovia del año 2016 la OTAN consideró oficialmente el ciberespacio como un nuevo dominio de las operaciones. Este hecho vino motivado por la evolución del panorama estratégico que se movía cada vez más en un entorno de conflictos híbridos. Al principio los ciberincidentes eran de pequeña índole y la reacción de la OTAN consistía en proteger sus redes y equipos. Pero estas acciones reactivas menores quedaron en evidencia en el ciberataque de 2007 contra Estonia. Lo cual supuso el despertar de la Alianza en materia de ciberseguridad (Fuente, 2022).

En abril de 2007 Estonia sufrió un ciberataque que paralizó las comunicaciones del país. Este ataque fue la consecuencia de la decisión del gobierno de Estonia de cambiar de ubicación la estatua del soldado de bronce, que era un remanente de la época de la Unión Soviética. El hecho provocó varios días de protestas y altercados y llegó a su punto más álgido con el ciberataque (Greenberg, 2019).

El ciberataque sufrido por Estonia supuso un antes y un después en el enfoque doctrinal de la OTAN. Para hacer frente a la nueva amenaza la Alianza ha ido desarrollando doctrina y ha creado diversas agencias y organismos como el Centro de Excelencia de Ciberdefensa Cooperativa (CCDCOE) en Tallin, la Agencia de Información y Comunicaciones (NCIA) o la División de Desafíos Emergentes de Seguridad (ESCD) (Fuente, 2022).

En España, el Jefe de Estado Mayor de la Defensa (JEMAD) promulgó la “Visión del JEMAD de la Ciberdefensa Militar”, en la que establece la Ciberdefensa como una nueva capacidad militar y considera las operaciones en el ciberespacio como operaciones permanentes debido a la naturaleza de la amenaza. Asimismo, establece que se deberá contar con las siguientes capacidades (EMAD, 2011a):

- Defensa: que incluya acciones de prevención, detección, reacción y recuperación frente a ataques.
- Explotación: orientada a la recopilación de información sobre sistemas de potenciales adversarios.
- Respuesta: con medidas contra amenazas o ataques.

Este documento llevó a la posterior promulgación del “Concepto de Ciberdefensa Militar del JEMAD”. El cual desarrolla la nueva capacidad y acota el ámbito de aplicación a los sistemas militares de mando y control e información. El documento desarrolla los principios, objetivos, funciones y responsabilidades, realizando también un estudio de viabilidad de la nueva capacidad en función a los aspectos MIRADO (Material, Infraestructura, Recursos humanos, Adiestramiento, Doctrina y Organización) (EMAD, 2011b).

Una vez definida la capacidad de ciberdefensa militar el JEMAD promulga el “Plan de Acción para la Obtención de la capacidad de Ciberdefensa Militar”. En él se identifican las acciones necesarias para la obtención de la capacidad de Ciberdefensa Militar (EMAD, 2012).

Posteriormente se crean el Mando Conjunto de Ciberdefensa (MCCD) en el año 2013 (posteriormente MCCE) y el Centro de Sistemas y Tecnologías de la Información y las Comunicaciones (CESTIC) en el año 2015. Doctrinalmente se publica la nueva “Política de sistemas de Información y Comunicaciones (CIS/TIC)” en el año 2015 así como la “Arquitectura Global CIS/TIC del Ministerio de Defensa” en el 2016. Por otro lado, el JEMAD promulga en el año 2018 el nuevo “Concepto de Empleo de las FAS”, que destaca la importancia del ciberespacio como un nuevo ámbito de seguridad. Todos estos cambios y la aparición de nuevos actores motivan la actualización en el año 2018 del “Concepto de Ciberdefensa”, que actualiza la doctrina existente y aborda la capacidad de ciberdefensa militar desde el punto de vista de la integración en el conjunto de las Fuerzas Armadas (FAS) y de otros actores civiles y militares del ámbito nacional e internacional. Así mismo identifica la necesidad de la integración de las capacidades de ciberdefensa en las operaciones militares conjuntas (EMAD, 2018).

Aparece por tanto una nueva forma de combatir en la que, al igual que en el resto de los dominios tradicionales, las operaciones de Inteligencia, Vigilancia y Reconocimiento (ISR) constituyen una capacidad esencial para anticiparse a las amenazas y proteger las redes y sistemas.

1.2 Problema y relevancia del estudio

Actualmente existe numerosa literatura técnica y doctrinal sobre ciberseguridad, pero cuesta encontrar referencias que aborden el análisis de las operaciones en el ciberespacio desde una perspectiva ISR (Intelligence, Surveillance and Reconnaissance) en su conjunto. Si bien existen múltiples marcos doctrinales y técnicos que abordan por separado aspectos como la vigilancia digital, el reconocimiento de infraestructuras o el ciclo de inteligencia de ciberamenazas, rara vez se integran de manera coherente en un modelo que los vincule de forma explícita con las operaciones militares en este dominio.

Esta situación genera un vacío doctrinal y metodológico que limita la capacidad de las Fuerzas Armadas para desarrollar operaciones ISR en el ciberespacio (CISRO) eficaces y coordinadas. La inexistencia de un marco operativo dificulta el planeamiento y la ejecución de este tipo de operaciones en el ciberespacio, especialmente en entornos híbridos y multidominio, donde las acciones ciber deben integrarse con las demás capacidades de la guerra convencional.

Desde el punto de vista académico, la relevancia de este estudio radica en la integración en un marco común del conocimiento actualmente disperso sobre cibervigilancia, reconocimiento e inteligencia de ciberamenazas, de manera que se comprenda los beneficios que aporta la realización de las operaciones ISR como un proceso unificado de obtención, análisis y explotación de la información en el dominio del ciberespacio.

En el plano práctico, la importancia de este trabajo radica en proponer un marco de referencia útil para la planificación y conducción de operaciones ISR que permitan lograr de una manera eficaz y eficiente la detección, anticipación y mitigación de amenazas en el ciberespacio.

En definitiva, el presente estudio busca contribuir a la comprensión y desarrollo de las operaciones ISR en el ciberespacio mediante un enfoque unificado que proporcione una base conceptual y metodológica sólida, orientada a fortalecer la capacidad operativa de las Fuerzas Armadas y a garantizar la superioridad de la información como elemento decisivo en el dominio del ciberespacio.

1.3 Objetivos

Los objetivos que se pretenden alcanzar son los siguientes:

Objetivo general (OG)

Revisar el estado del arte de las operaciones ISR en el ciberespacio y proponer una metodología que permita planificar y llevar a cabo este tipo de operaciones, identificando su marco doctrinal, así como sus procedimientos técnicos.

Objetivos específicos (OE)

OE1: Describir el marco conceptual y doctrinal de las operaciones en el ciberespacio, atendiendo a su reconocimiento como dominio en las operaciones militares y a la organización de las capacidades en el ciberespacio a nivel nacional e internacional.

OE2: Adaptar el ciclo de la inteligencia clásica al ámbito del ciberespacio siguiendo el enfoque de la inteligencia de ciberamenazas (CTI).

OE3: Estudiar las técnicas de análisis estructurado que mejor se adecuen al análisis de la inteligencia obtenida de los ciberataques.

OE4: Analizar las técnicas y metodologías de cibervigilancia orientadas a la monitorización de actores y amenazas en el ciberespacio.

OE5: Examinar las técnicas de reconocimiento en el ciberespacio, tanto pasivas como activas, aplicadas a infraestructuras y personas para obtener un procedimiento ordenado que guíe a la obtención de la superficie de exposición y la identificación de potenciales vectores de ataque.

1.4 Metodología

La metodología seguida en este trabajo responde a un enfoque analítico orientado a la revisión de doctrinas, marcos conceptuales y técnicas relacionadas con las operaciones ISR en el ciberespacio. El estudio se apoya en el examen de documentación académica, normativa e institucional de organismos nacionales e internacionales, complementada con literatura técnica especializada en los ámbitos de la inteligencia de ciberamenazas, la cibervigilancia y el reconocimiento en el ciberespacio. Todo ello orientado y guiado por la experiencia profesional propia del autor en esta materia.

En primer lugar, se realiza una revisión bibliográfica y documental que incluye doctrinas militares (OTAN, UE, Estados Unidos y España), la estrategia nacional de ciberseguridad, informes de agencias especializadas como ENISA, publicaciones académicas recientes en el campo de la ciberdefensa y las principales leyes nacionales e internacionales que dan cabida a las operaciones ISR en el ciberespacio. Esta revisión tiene como finalidad establecer el marco teórico y conceptual en el que se inserta el presente trabajo.

En segundo lugar, se analizan cada una de las capacidades que integran las operaciones ISR en el ciberespacio, tratando de ofrecer un enfoque ordenado y secuencial de las acciones que pueden realizar de manera que sirvan de guía o procedimiento a seguir. En los conceptos más abstractos, para facilitar la comprensión del lector, se muestran ejemplos básicos y conceptuales de elaboración propia del autor.

Para lograr el objetivo del trabajo se adopta un enfoque sintetizador, directo e integrador, tratando de identificar las tareas a realizar y ordenarlas de una manera coherente de manera que proporcionen al lector una visión clara de la aportación de las operaciones ISR, así como una metodología a seguir para poder planearlas o llevarlas a cabo.

1.5 Estructura

El presente trabajo se articula en siete capítulos que siguen un orden lógico que permite avanzar desde la contextualización inicial hasta el análisis específico de las operaciones ISR en el ciberespacio.

Capítulo 1. Introducción.

Se presentan el contexto general, la relevancia del tema, el problema de investigación y los objetivos del estudio. Asimismo, se expone la metodología adoptada y se describe la organización del trabajo.

Capítulo 2. Estado del arte.

Este capítulo examina el marco doctrinal y conceptual que sustenta el estudio, abordando la definición del ciberespacio y la organización de las capacidades ciber. También se revisan los principales tipos de operaciones, sus efectos y las consideraciones legales asociadas a las operaciones ISR, tema principal del trabajo.

Capítulo 3. Inteligencia

Se desarrolla el ciclo de inteligencia aplicado al ciberespacio (inteligencia de ciberamenazas), análisis de modelos y metodologías de referencia como MITRE ATT&CK, Kill Chain o Diamond Model, así como la presentación de los principales estándares de compartición de información.

Capítulo 4. Cibervigilancia

Se estudian las técnicas y metodologías de monitorización de amenazas, fugas de información, actividades hacktivistas, así como las diferentes disciplinas de obtención y los ámbitos de actuación en la red.

Capítulo 5. Reconocimiento

Se analizan los procedimientos pasivos y activos aplicados a infraestructuras y personas, orientados a la obtención de la superficie de exposición, vectores de ataque y enumeración interna de sistemas.

Capítulo 6. Conclusiones.

Se sintetizan los principales hallazgos del trabajo, se evalúa la aportación del enfoque ISR a la seguridad en el ciberespacio, y se proponen posibles líneas de investigación futuras.

Capítulo 7. Bibliografía.

Incluye todas las referencias bibliográficas y documentales utilizadas, siguiendo el estilo de citación académica normalizado APA 7.

2 ESTADO DEL ARTE

2.1 Ciberespacio

Se puede entender el ciberespacio como el entorno virtual global donde se relacionan diversos elementos como servicios de Internet, datos, usuarios, redes, líneas de comunicación, etc. (ESFAS, 2014).

El ciberespacio está comprendido por tres capas (física, lógica y social) (Figura 2-1), las cuales comprenden componentes geográficos, redes físicas, redes lógicas, ciber personas y personas (acqnotes, s.f).

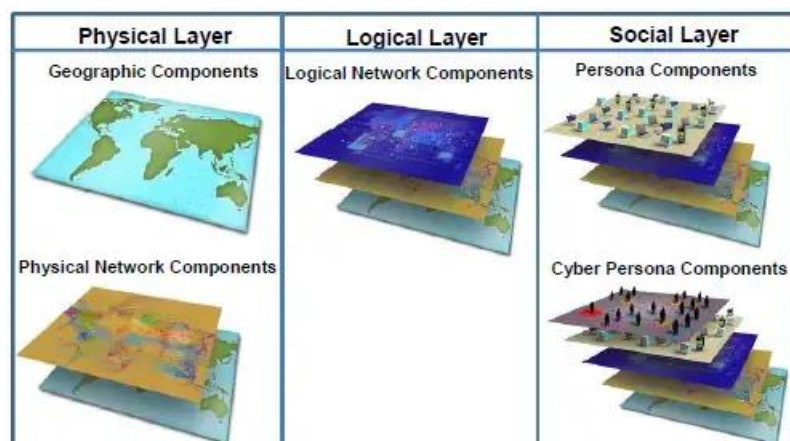


Figura 2-1 Capas que comprenden el ciberespacio (acqnotes, s.f)

Capa física: La capa física incluye los componentes geográficos y las redes físicas. Se entiende como componente físico a la localización de los elementos de una red. Por otro lado, las redes físicas se componen de hardware e infraestructura (cableada, inalámbrica y óptica).

Capa lógica: La capa lógica comprende los componentes lógicos de red, así como las conexiones lógicas entre los nodos. Los nodos son dispositivos conectados a la red como ordenadores, teléfonos, etc. Podríamos decir que un nodo es un dispositivo con una dirección IP asignada.

Capa social: La capa social engloba los aspectos humanos cognitivos, incluyendo personas y ciber personas. Se entiende como ciber persona la identificación de la persona en la red (avatar, correo electrónico, número de teléfono, dirección IP, etc.). La persona se considera como parte de la red y puede tener asociadas varias ciber personas como p. ej., varios correos electrónicos. Así mismo una ciber persona puede asociarse a múltiples usuarios. Es el caso de varios usuarios con acceso a un buzón de correo corporativo (acqnotes, s.f.).

Según (DSN, 2019) el ciberespacio presenta por sí mismo unas características inherentes que le diferencian de otros dominios tradicionales como el marítimo, terrestre o aéreo. Estas son:

- Ausencia de soberanía.
- Facilidad de acceso.
- Dificultad de atribución de acciones.
- Débil jurisdicción.

Estas características posibilitan el uso malicioso o fraudulento del ciberespacio, presentando una serie de amenazas asociadas (Figura 2-2), que, atendiendo a la Estrategia Nacional de Ciberseguridad podemos categorizar como (DSN, 2019):

- **Ciberspionaje.** Robo malicioso de información a través de sistemas informáticos normalmente realizado por Estados mediante grupos organizados denominados Amenaza Persistente Avanzada (APT). (Fortinet, 2025).
- **Amenazas híbridas.** Combinan medios militares y civiles que actúan en modos encubierto o abierto. En esta categoría se encuentran la desinformación, ciberataques, presión económica, presión migratoria, etc. (NATO, 2024b).
- **Cibercrimen.** Actividades delictivas contra ordenadores o redes informáticas con el objetivo de provocar daños a estos sistemas o la obtención de beneficio económico. Esta categoría comprende numerosos tipos de actividades maliciosas, siendo los más comunes los siguientes (EUROPOL, s.f.; Kaspersky, s.f.):
 - Fraude por correo electrónico e Internet.
 - Robo de datos.
 - Ciberextorsión.
 - Ataques de ransomware.
 - Minería de criptomonedas empleando recursos ajenos (Cryptojacking).
 - Pornografía infantil.
- **Hacktivismo.** Es la ejecución de acciones activistas en el ciberespacio. Se realiza mediante ataques informáticos que reivindican una causa, normalmente política, social o económica. Existen grupos hacktivistas con diferentes motivaciones, ideologías y tendencias políticas (UNIR, 2021).



Figura 2-2 Ciberamenazas y acciones que utilizan el ciberespacio con fines maliciosos (DSN, 2019)

2.2 Estructura y organización de un Mando militar ciber

Para llevar a cabo las operaciones en el ciberespacio un Mando ciber debe disponer de una estructura modular y funcional que le permita cumplir con sus cometidos de una manera eficaz. La organización de un Mando ciber (Figura 2-3) no difiere de la organización de cualquier otro Mando componente, apareciendo como elementos de maniobra unidades propiamente ciber (CCDCOE, 2020).

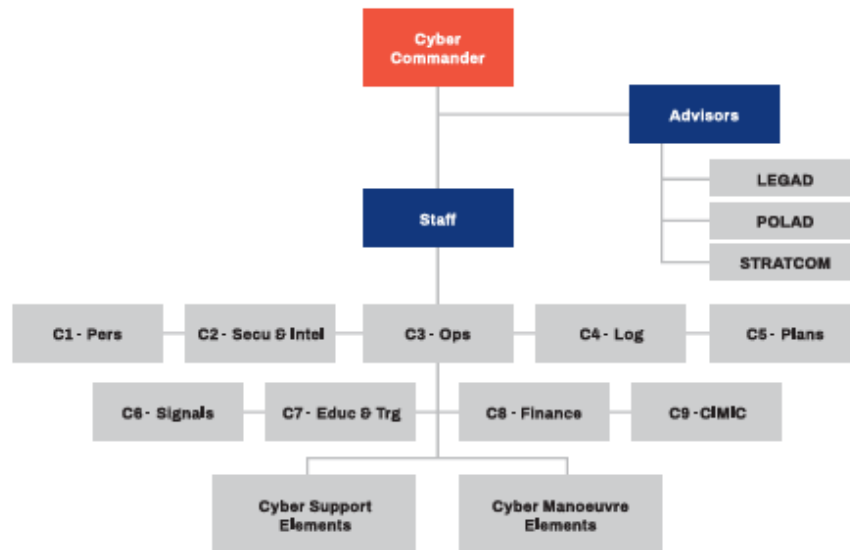


Figura 2-3 Organización tipo de un Mando Ciber (CCDCOE, 2020)

Los elementos de maniobra ciber son las unidades operativas que ejecutan las ciberoperaciones. Doctrinalmente la OTAN establece las siguientes unidades (CCDCOE, 2020):

2.2.1 Security Operations Centre (SOC)

El Security Operations Centre (SOC) o Centro de Operaciones de Seguridad (COS), es la unidad encargada de monitorizar las redes para detectar, analizar, responder y prevenir los incidentes de ciberseguridad. Los integrantes de esta unidad realizan un triaje y estudio somero de las alertas sin entrar en profundidad en los incidentes. Cuando un incidente requiere de mayor atención se escala al CERT. En la Figura 2-4 se pueden ver las funciones habituales de un SOC.



Figura 2-4 Funciones de un SOC (Comodo, s.f.)

2.2.2 Computer Emergency Team (CERT)

El CERT o Computer Emergency Team es un equipo de expertos que tienen la misión del análisis en profundidad de ciber incidentes. Un CERT provee de capacidades adicionales a las que ofrece un SOC (Figura 2-5), como pueden ser el análisis forense, respuesta a incidentes, gestión de vulnerabilidades, y el adiestramiento y concienciación.

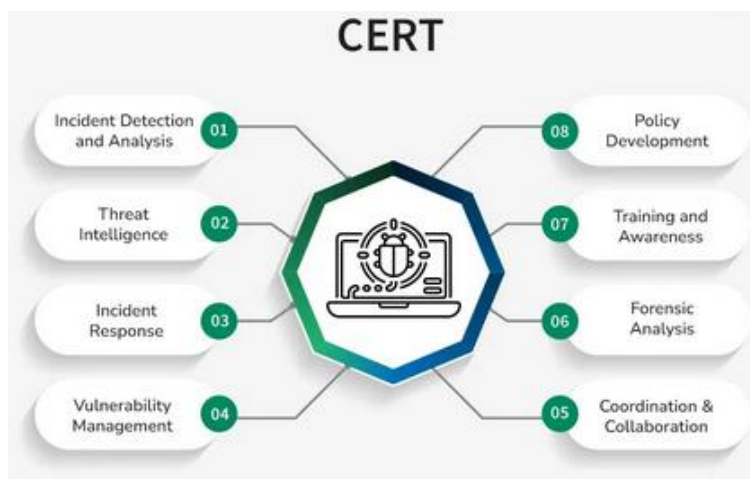


Figura 2-5 Funciones de un CERT (GeeksforGeeks, 2024)

2.2.3 Rapid Reaction Team (RRT)

Los Rapid Reaction Team (RRT) en ámbito OTAN o los Equipos de Respuesta a Incidentes de Seguridad (ERI) en ámbito nacional son equipos desplegables de expertos preparados para acudir rápidamente al lugar donde haya ocurrido un ciber incidente y la asistencia en remoto no sea una opción. Suelen tener un periodo de activación de alerta de 72 horas y la composición de los equipos varía en función del tipo de incidente al que tengan que acudir (CCDCOE, 2020; CCN, 2021).

2.2.4 Elementos de enlace

Al igual que en otros dominios o ejércitos, el ciberespacio debe ser tenido en cuenta en todas las operaciones, así como en los planeamientos. Para ello es fundamental que exista un oficial de enlace ciber que actúe como experto en la materia y que asesore y coordine en asuntos ciber.

2.3 Tipos de ciberoperaciones

En el dominio del ciberespacio actualmente se reconocen cuatro tipos de operaciones (CCDCOE, 2020; NATO, 2020) (Figura 2-6):

- Communications and Information Systems Infrastructure Operations (CISIO).
- Defensive Cyber Operations (DCO).
- Offensive Cyber Operations (OCO).
- Cyberspace Intelligence, Surveillance and Reconnaissance Operations (CISRO).

Estos tipos de actividades tienen unas características que se desarrollan a continuación:

2.3.1 CISIO

Las operaciones de infraestructuras CIS¹ tienen la misión de asegurar la ciber resiliencia, concienciación y apoyo a las unidades que lo necesiten. Normalmente estas operaciones recaen en las secciones CIS de los Estados Mayores. En este tipo de operación entran en juego los siguientes equipos (CCDCOE, 2020):

- Equipos de auditoría: comprueban la correcta aplicación de las medidas de seguridad en los sistemas CIS, son responsables de:
 - Guiar y aconsejar en la aplicación de directivas y políticas de ciberseguridad.
 - Revisar y aprobar la documentación de seguridad.
 - Acreditar sistemas.
- Equipos de análisis de vulnerabilidades: realizan:
 - Escaneos de vulnerabilidades.
 - Test de seguridad y evaluación para comprobar que los sistemas están correctamente securizados.
- Equipos de evaluación de ciberseguridad: realizan:
 - Tests de penetración (PENTEST).
 - Test de comprobación de las mejoras acordadas en los informes de auditoría.

2.3.2 DCO

Según NATO (2020) las operaciones DCO se definen como acciones defensivas realizadas en o a través del ciberespacio y que tienen como finalidad preservar la libertad de acción en el ciberespacio. Estas operaciones incluyen acciones encaminadas a prevenir, mitigar o responder las operaciones adversarias en el ciberespacio. Las DCO no solo protegen las redes y sistemas, también la información contenida en ellos.

Normalmente este tipo de operaciones se conducen sobre redes y sistemas propios, aunque en ocasiones se realizan en apoyo de otros organismos estratégicos. Este es el caso de operaciones de apoyo a organismos civiles como, p.ej., la integración del Mando Conjunto del Ciberespacio (MCCE) en los dispositivos de seguridad de los procesos electorales (Ruiz, 2024).

Para cumplir su misión, las DCO comprenden varias capacidades entre las que se encuentran (Blanco, 2021):

- Monitorización: instalación de sondas en las redes a vigilar y análisis de logs.
- Correlación de eventos: gestión de alertas en sistemas SIEM² para detectar incidentes de seguridad.
- Gestión de incidentes: equipos especializados en la resolución de los incidentes.
- Análisis forense: análisis en profundidad de dispositivos afectados por un incidente.
- Threat Hunting: búsqueda de amenazas conocidas en redes propias en base a indicadores de compromiso (IOC) y Tácticas, Técnicas y Procedimientos (TTP) conocidos (Ikusi, s.f.).

¹ Communications & Informations Systems

² Security Information and Event Management. Es un Sistema que combina la Gestión de Información de Seguridad (SIM) y la Gestión de Eventos de Seguridad (SEM).

2.3.3 OCO

Las ciberoperaciones ofensivas comprenden las acciones en o a través del ciberespacio para crear efectos que permitan cumplir con objetivos militares. Las OCO pueden realizarse por sí mismas o como parte de otro tipo de operaciones militares (NATO, 2020).

La doctrina de EE. UU. contempla dos tipos de OCO (Moore, 2021):

- **Presence-based operations:** actividades ofensivas orientadas a mantener una permanencia en las redes adversarias.
- **Event-based operations:** acciones ofensivas directas con el objetivo de causar efectos inmediatos en los sistemas del adversario.

La OTAN no contempla el desarrollo de capacidades ofensivas en ninguno de los dominios en los que opera. Además, debido a la clasificación de seguridad que conlleva la realización de operaciones de tipo OCO y a que los países son reacios a compartir información y sus TTP, la OTAN introdujo el mecanismo SCEPVA³ (Goździewicz, 2019). Con este mecanismo la Alianza se beneficia de los ciber efectos producidos por las naciones, pero no asigna OCO a ninguna nación. Cuando operacionalmente se tiene la necesidad de conseguir un efecto ciber sobre un target, se recurre a los países miembros del mecanismo SCEPVA que estén dispuestos a acometer ese target con una OCO. Todo ello se realiza cumpliendo con las reglas de enfrentamiento de la operación OTAN en curso. La coordinación de las OCO las realiza el NATO's Cyberspace Operations Centre (CyOC) (CCDCOE, 2020).

2.3.4 CISRO

Las operaciones ISR en el ciberespacio (CISRO) están orientadas a la obtención de inteligencia a través del ciberespacio. Las operaciones de obtención pueden ser intrusivas y no intrusivas (CCDCOE, 2020):

- **Operaciones no intrusivas:** la información se obtiene desde las redes propias o realizando inteligencia de fuentes abiertas (OSINT) sobre redes adversarias o ajenas.
- **Operaciones intrusivas:** la obtención se realiza sobre redes adversarias o ajenas en las que no está disponible la información. Este tipo de obtención contempla el compromiso de sistemas y la exfiltración de información.

Las operaciones CISRO se centran en el estudio de las Tácticas, Técnicas y Procedimientos del adversario, así como a la obtención de vulnerabilidades y vectores de ataque. Además, como en los demás dominios del campo de batalla, contribuyen al estudio y análisis del entorno operacional según las variables PMESII (Romford, 2025):

- Política.
- Militar.
- Económica.
- Social.
- Información.
- Infraestructura.

³ Sovereign Cyber Effects Provided Voluntary by Allies

Las CISRO comprenden tres capacidades, Inteligencia (Intelligence), Vigilancia digital (Surveillance) y Reconocimiento (Reconnaissance), las cuales se desarrollan con un enfoque metodológico en este TFM.

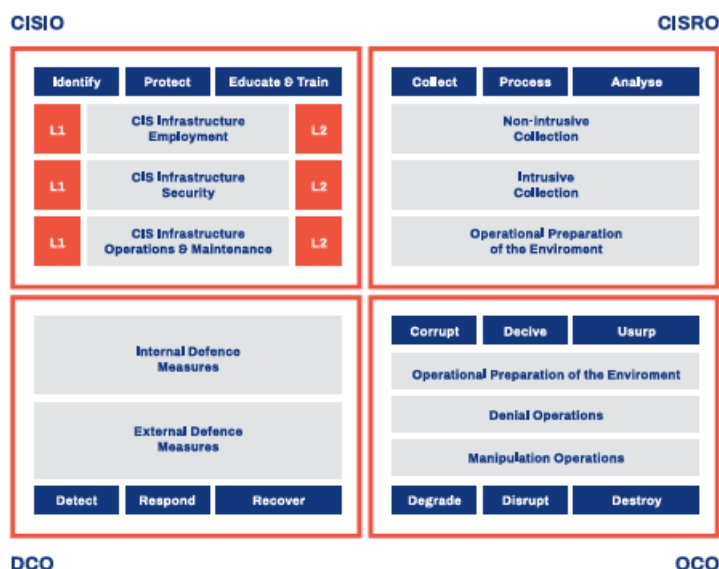


Figura 2-6 Framework de operaciones en el ciberespacio (CCDCOE, 2020)

2.4 Efectos

De cara al planeamiento de una ciberoperación, la OTAN contempla los siguientes efectos (NATO, 2020):

- **Securizar.** Prevenir que el adversario ponga en riesgo la triada de Confidencialidad, Integridad y disponibilidad (CIA) en las redes y sistemas a proteger.
- **Aislar.** Bloquear las líneas de comunicación entre el adversario y su código o actividad maliciosa dentro de los sistemas afectados.
- **Contener.** Impedir que se siga propagando el código o actividad maliciosa.
- **Neutralizar.** Hacer que el código o la actividad maliciosa sean permanentemente incapaces de seguir afectando a la CIA⁴ de las redes y sistemas a proteger.
- **Recuperar.** Eliminar y mitigar los efectos del código o la actividad maliciosa en los sistemas afectados para restaurar la funcionalidad.
- **Manipular.** Controlar, modificar o comprometer la integridad de la información, los sistemas y/o las redes del adversario cumpliendo los objetivos del comandante de la operación.
- **Exfiltrar.** Recopilar, descargar o robar información mediante acceso no autorizado.
- **Degradar.** Denegar el acceso o la operación de un sistema o red a un nivel reducido de su capacidad o rendimiento. Normalmente se especifica un nivel de reducción deseado.
- **Interrumpir.** Denegar completamente el acceso o la operación de un activo durante un período determinado. Normalmente se especifica una hora de inicio y una hora de finalización deseadas. La interrupción puede considerarse un caso especial de degradación donde el nivel de degradación seleccionado es del 100 % durante un período determinado.

⁴ Confidentiality, Integrity & Availability

- **Destruir.** Negar total e irreparablemente el acceso o la operación de un activo. El activo se ve afectado al máximo, tanto en términos de tiempo de interrupción como de daños.

2.5 Consideraciones legales en las operaciones CISRO

Las operaciones militares se planean y ejecutan cumpliendo siempre unas Reglas de Enfrentamiento (ROE) orientadas a la misión que establecen al comandante de la operación unas orientaciones claras sobre el uso de la fuerza o de otras acciones que puedan llegar a considerarse como provocativas contra otros actores en el área de operaciones. Estas reglas de enfrentamiento deben estar siempre amparadas en la legislación nacional e internacional (CCDCOE, 2020).

La legislación internacional establece que las naciones no pueden operar en otro estado sin su consentimiento o sin una base legal o mandato internacional. Esta prohibición se sustenta en tres principios: principio de no intervención, principio de soberanía y la prohibición del uso de la fuerza en las relaciones internacionales. En caso de conflicto se aplicará el Derecho Internacional Humanitario. En el ciberespacio las operaciones suelen traspasar las fronteras nacionales. En este sentido el desarrollo de operaciones fuera de las fronteras nacionales está regulado por la legislación internacional y por la nacional (CCDCOE, 2020). Con el Manual de Tallin (Figura 2-7), el Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN (CCDCOE) ha desarrollado doctrina al respecto, que, aunque no es jurídicamente vinculante, da una interpretación de cómo se aplica el Derecho Internacional Humanitario a los conflictos en el ciberespacio (Schmitt, 2017).

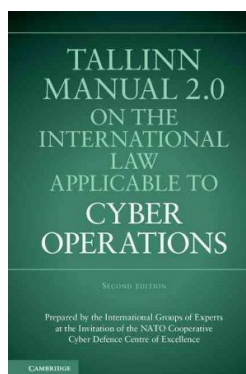


Figura 2-7 Manual de Tallin 2.0 (Securityaffairs, 2017)

Particularizando en las ciberoperaciones ISR intrusivas, al tratarse de operaciones de inteligencia, tienen una consideración diferente a una acción ofensiva (OCO) que cause unos efectos en el objetivo. El ciberespionaje en conflictos armados o en tiempos de paz no está contemplado en la legislación internacional. El Manual de Tallin sugiere que el ciberespionaje puede ser ilegal si vulnera la soberanía de otro Estado o implica interferencia en asuntos internos, aunque no se debe olvidar que este manual no es un texto jurídico vinculante (Schmitt, 2017). En este sentido la Convención de Budapest, en su artículo 2, indica que este tipo de acciones se juzgarán aplicando la legislación nacional (Wegener, 2013).

En España estas operaciones están asignadas a unos organismos concretos y están amparadas en base a las siguientes leyes:

- Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI). Asigna al CNI la misión de obtener información relevante para prevenir amenazas a la seguridad, soberanía e integridad de España (Ley 11/2002, 2002).
- Ley Orgánica 5/2005, de la Defensa Nacional. Establece que las Fuerzas Armadas pueden ser empleadas para proteger los intereses de España también en el ciberespacio y fuera del territorio nacional. En este contexto el Ministerio de Defensa y el Mando Conjunto del Ciberespacio

(MCCE) pueden participar en operaciones de este tipo, ya sean de carácter nacional como en operaciones conjuntas dentro de la OTAN o UE (Ley Orgánica 5/2005, 2005).

- La Orden DEF/1110/2023, de 4 de octubre, por la que se desarrolla la organización básica del Estado Mayor de la Defensa asigna al MCCE, en concreto a la Fuerza de Operaciones en el Ciberespacio (FOCE) la responsabilidad de la ejecución de ciberoperaciones para garantizar la libertad de acción de las Fuerzas Armadas (Ministerio de Defensa de España, 2023).
- Estrategia de Ciberseguridad Nacional (2019). Reconoce que España puede disponer de capacidades de ciberinteligencia ofensiva (DSN, 2019).

Si las operaciones de ciberespionaje se llevan a cabo por particulares o entidades españolas sin autorización se aplicará la legislación española al respecto. La constitución española en los artículos 17, 18 y 24 garantiza los derechos fundamentales de privacidad, protección de datos y secreto de las comunicaciones salvo que se actúe bajo una resolución judicial. El ámbito legislativo se ha ido adaptando poco a poco a la aparición de acciones en el ciberespacio modificando el Código Penal para incluir ciberdelitos y desarrollando una serie de leyes, relacionándose a continuación las más destacadas (Álvarez, 2019):

- Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD). Es la adaptación nacional del Reglamento General de Protección de Datos de la UE y regula el tratamiento de datos personales en entornos digitales (Ley Orgánica 3/2018, 2018).
- Código Penal (Título XIII bis – Delitos Informáticos). Regula los delitos informáticos como el acceso ilícito a sistemas informáticos, interceptación de comunicaciones, revelación de secretos o espionaje industrial. Los artículos que aplican son (Ley Orgánica 10/1995, 1995):
 - Art. 197: Descubrimiento y revelación de secretos.
 - Art. 197 bis y 197 ter: Acceso y uso de sistemas informáticos sin autorización.
 - Art. 278-280: Espionaje empresarial e industrial.

3 INTELIGENCIA

Al igual que en el resto de los ámbitos clásicos, en el ciberespacio se recibe una ingente cantidad de información de diversa índole. Antes de desarrollar el concepto de inteligencia y en concreto la inteligencia de ciberamenazas conviene definir el concepto de información, que consiste en los datos obtenidos sin elaborar ni analizar y que son susceptibles de ser empleados en la producción de inteligencia (EMAD, 2020).

Según EMAD (2020) la inteligencia se puede definir como el resultado de la obtención, análisis y elaboración de la información. Dicho de otra manera, la inteligencia se puede considerar como los datos analizados en un contexto determinado (Figura 3-1).

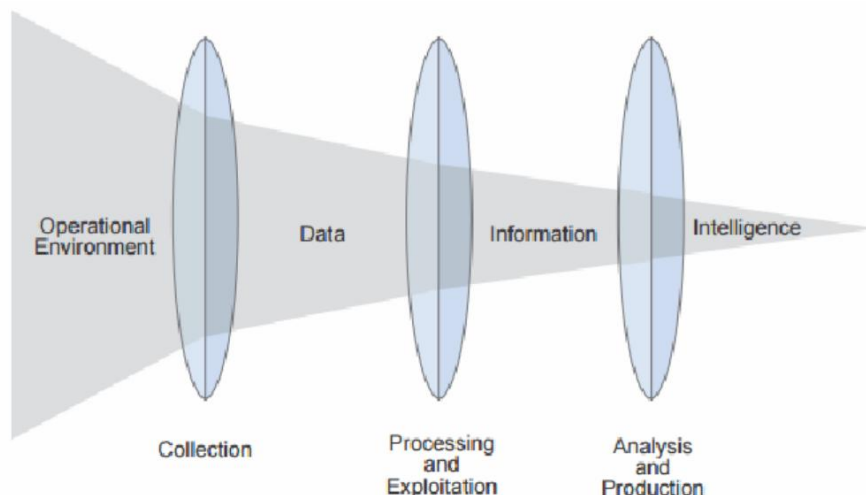


Figura 3-1 Relación entre datos, información e inteligencia (Huarui, 2022)

En el ámbito del ciberespacio, la inteligencia se caracteriza como inteligencia de ciberamenazas o Cyber Threat Intelligence (CTI), en adelante CTI, que es la inteligencia orientada a entender la motivación, objetivos y métodos de ataque de los actores amenaza (Baker, 2025a).

En función del consumidor objetivo, la inteligencia de ciberamenazas se clasifica en cuatro áreas (Figura 3-2) (Baker, 2025a; Guerra, 2023; Recorded Future, 2022):

- **Estratégica:** orientada a las tendencias y motivaciones de los adversarios con el objetivo de ayudar en la toma de decisiones a alto nivel. Los consumidores son el nivel de dirección (CISO, CIO y Mandos estratégicos en las Fuerzas Armadas).
- **Operacional:** centrada en estudiar las capacidades, infraestructura, así como las Tácticas, Técnicas y Procedimientos de los adversarios. Identifica y analiza campañas y acciones de potenciales actores de amenaza contra la organización. Está orientada a los analistas de SOC, Threat Hunters, forenses, equipos de respuesta a incidentes, etc.
- **Táctica:** analiza las TTP de los atacantes para entender cómo realizan sus ataques. Los principales consumidores de este tipo de inteligencia son el personal de los SOC, arquitectos de seguridad, personal de respuesta a incidentes, etc.
- **Técnica:** proporciona información técnica a más bajo nivel como los indicadores de compromiso (IOC) y demás recursos que dispone el atacante y que ayuda a la detección en las redes de la organización de ataques en curso que estén ocurriendo en otras organizaciones. Los productos de inteligencia están orientados al personal del SOC y al de respuesta a incidentes.



Figura 3-2 Tipos de inteligencia de ciberamenazas según la audiencia objetivo (Guerra, 2023)

Para producir productos de inteligencia que satisfagan las necesidades de los diferentes tipos de audiencia objetivo se sigue el ciclo de inteligencia, que es el proceso circular que hace posible la obtención de los datos y su transformación en inteligencia accionable y procesable. El Ministerio de Defensa de España establece cuatro fases para este ciclo (Figura 3-3) que son las siguientes (EMAD, 2020):

- **Dirección.** Se identifican objetivos y necesidades de información.
- **Obtención.** Recolección de información mediante las distintas disciplinas de obtención de la inteligencia (OSINT⁵, SIGINT⁶, HUMINT⁷, VHUMINT⁸, etc.).
- **Elaboración.** Se analizan, procesan y convierten los datos obtenidos en inteligencia accionable.
- **Difusión.** Se comparten los productos de inteligencia con los organismos consumidores de esta inteligencia.



Figura 3-3 Fases del ciclo de inteligencia (EMAD, 2020)

⁵ Open Source Intelligence

⁶ Signal Intelligence

⁷ Human Intelligence

⁸ Virtual Human Intelligence

A continuación, se propone una metodología ordenada que sigue cada una de las fases anteriormente mencionadas y se presentan algunas técnicas que pueden servir de procedimiento o guía para los analistas.

3.1 Fase de Dirección

3.1.1 Modelado de amenazas

En primer lugar, el Mando o la Dirección debe saber a quién y a qué se enfrenta. Para ello debe determinar los activos críticos de la organización (información y sistemas), conocer las amenazas y determinar los potenciales atacantes. Este proceso se denomina modelado de amenazas y conlleva una serie de fases (Guerra, 2023):

- **Establecer los objetivos.** Por ejemplo, preservar la Confidencialidad, Integridad y disponibilidad (CIA) de los activos de la organización.
- **Visualización.** Inventariar los activos de la organización. Véase Figura 3-4.

ACTIVO	DUEÑO DEL ACTIVO	DUEÑO DEL RIESGO	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	VALOR
CPD	Dpto. Sistemas	Dirección	4	3	5	5
Empleados	Dpto. RRHH	Dirección	3	2	3	3
Datos personales de los clientes	Dpto. Sistemas, Dpto. Jurídico	Dirección	5	4	3	5
Datos internos de la empresa	Dpto. Sistemas, Dpto. Operaciones	Dirección	3	3	3	3
Software de venta al cliente (APP)	Dpto. Sistemas	Dirección	3	4	5	5
Software adquirido para la gestión de la empresa	Dpto. Sistemas	Dirección	2	3	3	3
Servidor WEB	Dpto. Sistemas	Dirección	2	2	5	5
Servidor de ficheros	Dpto. Sistemas	Dirección	4	4	5	5
Terminales de usuario	Dpto. Sistemas	Dirección	2	2	3	3
Elementos comms perimetrales	Dpto. Sistemas	Dirección	3	3	5	5

Figura 3-4 Inventariado y valoración de los activos de una organización (elaboración propia)

- **Identificación de amenazas.** Análisis de las vulnerabilidades y amenazas contra los activos (P. ej., superficie de exposición) y estudio de posibles atacantes.

Para el estudio de los posibles atacantes se tiene en cuenta el sector de actividad de la organización, así como factores motivacionales, políticos o estratégicos. Por ejemplo, como se observa en la Figura 3-5, si la organización es un banco, los potenciales atacantes serán los grupos APT dedicados al sector financiero, si es el Ministerio de Defensa, serán los grupos APT de los países hostiles.

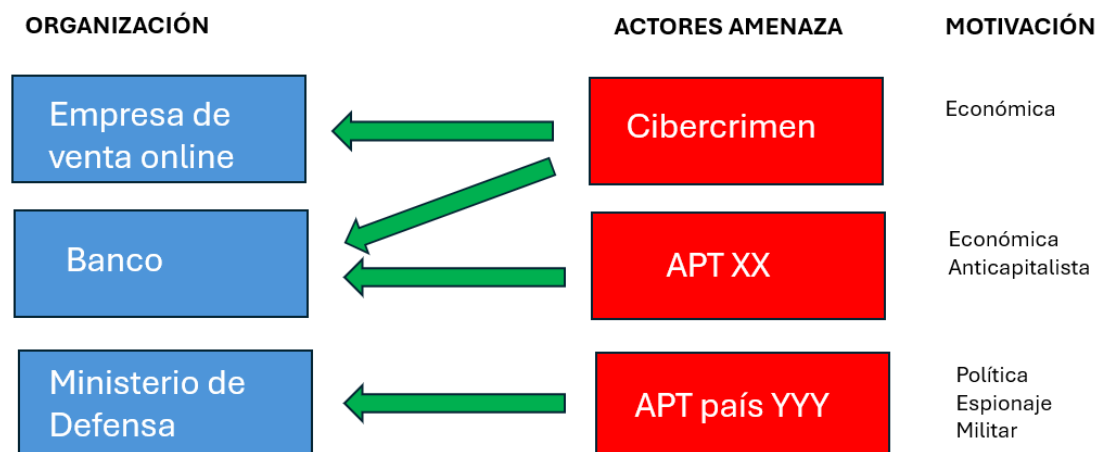


Figura 3-5 Modelado de la amenaza a nivel estratégico (elaboración propia)

- **Mitigación.** En esta fase se realizará un análisis de riesgos de las vulnerabilidades identificadas en la fase anterior, tomando la decisión adecuada con cada una de ellas: asumir, reducir, transferir o evitar. Véase la Figura 3-6.

ACTIVO	RIESGO											MAXIMO	Nivel de riesgo
	Fuego	Fallo del servicio de comunicaciones	Temperatura	Corte del suministro eléctrico	Denegación de servicio	Alteración de la información	Errores de administrador/usuario	Difusión de software dañino	Ataques de una organización criminal	Robo	Abuso de privilegios de acceso		
CPD	25	60	50	60	5	5	5	5	5	25	20	60	Alto
Empleados	6	3	9	3	3	3	12	3	3	3	3	12	Bajo
Datos personales de los clientes	25	30	40	20	20	25	30	75	50	50	75	75	Alto
Datos internos de la empresa	25	30	40	20	10	25	30	75	50	40	60	75	Alto
Software de venta al cliente (APP)	15	60	40	20	20	25	30	75	50	25	45	75	Alto
Software adquirido para la gestión de la empresa	16	48	32	48	4	20	24	60	60	12	24	60	Alto
Servidor WEB	25	75	60	60	75	15	45	75	75	25	75	75	Alto
Servidor de ficheros	25	75	60	60	20	25	30	50	75	25	50	75	Alto
Terminales de usuario	15	36	36	36	12	9	18	36	36	9	27	36	Medio
Elementos comms perimetrales	25	75	60	60	75	5	60	45	45	25	75	75	Alto

Figura 3-6 Análisis de riesgos de una organización (elaboración propia)

- **Validación.** Comprobación de que se han solventado las vulnerabilidades encontradas y seguimiento de los riesgos residuales.

3.1.2 Necesidades de información

Una vez se conoce la amenaza el Mando o Dirección de la organización debe determinar las necesidades de información y proporcionar a los equipos de inteligencia instrucciones claras y precisas de lo que necesita conocer. Estas necesidades se estructuran de la siguiente manera (EMAD, 2020):

- **Necesidades Críticas de Información del Comandante (CCIR).** Son los conocimientos clave que un comandante debe tener para garantizar que la misión asignada pueda cumplirse con éxito. Se trata de preguntas muy concretas, normalmente de respuesta tipo si/no, y cuya contestación condicionará el planeamiento de la operación.
- **Necesidades Prioritarias de Inteligencia (PIR).** Constituyen la parte de las CCIR que el Mando identifica como más relevantes para llevar a cabo un buen planeamiento y toma de decisiones.

- **Necesidades Específicas de Inteligencia (SIR).** Detallan de manera más concreta la información necesaria para responder a cada necesidad prioritaria de Inteligencia.
- **Elementos Esenciales de Información (EEI).** Surgen de desglosar las SIR en aspectos más precisos, proporcionando el nivel de detalle adecuado para poder elaborar el Plan de Obtención.

Sirva como ejemplo las siguientes tablas (Tabla 3-1, Tabla 3-2 y Tabla 3-3) en las que se puede ver cómo serían las necesidades de información en función del nivel de la audiencia (estratégico, operacional y táctico):

CCIR	PIR	SIR	EEI
1. ¿El país XX tiene capacidades en ciberdefensa maduras?	1.1 ¿Cuáles son las capacidades ciber del país XX?	1.1.1 ¿Cuáles son las capacidades ofensivas del país XX?	1.1.1.1 Capacidad de desarrollo de malware
			1.1.1.2 Grupos APT
			1.1.1.3 Conocimientos en sistemas SCADA ⁹
		1.1.2 ¿Cuáles son las capacidades defensivas del país XX?	1.1.2.1 Sistemas SIEM
			1.1.2.2 Capacidad forense

Tabla 3-1 Necesidades de información a nivel estratégico (elaboración propia)

CCIR	PIR	SIR	EEI
1. ¿El país XX tiene experiencia realizando operaciones ciber ofensivas?	1.1 ¿Qué ciberoperaciones ofensivas ha llevado a cabo el país XX?	1.1.1 ¿Qué capacidades específicas utilizó el país XX?	1.1.1.1 Vulnerabilidades explotadas
			1.1.1.2 Infraestructura empleada
		1.1.2 ¿Qué objetivo atacó el país XX?	1.1.2.1 Tipo de red atacada
			1.1.2.2 Efectos conseguidos en el objetivo

Tabla 3-2 Necesidades de información a nivel operacional (elaboración propia)

CCIR	PIR	SIR	EEI
------	-----	-----	-----

⁹ Supervisory Control and Data Acquisition: sistema de supervisión y recopilación de datos en tiempo real de procesos industriales.

1. ¿La red de Mando y Control es atacable desde el exterior?	1.1 ¿Qué superficie de exposición tiene la red de Mando y Control?	1.1.1 Puntos de acceso desde el exterior	1.1.1.1 Puertos abiertos y servicios
			1.1.1.2 Formularios de entrada web
			1.1.1.3 Correos electrónicos
		1.1.2 Vulnerabilidades	1.1.2.1 CVEs
			1.1.2.2 Fallos de configuración
		1.1.3 Seguridad de la red	1.1.3.1 Antivirus, EDR ¹⁰ , XDR ¹¹
			1.1.3.2 Sistemas de monitorización SIEM

Tabla 3-3 Necesidades de información a nivel táctico (elaboración propia)

3.1.3 Plan de obtención

Una vez modelada la amenaza y determinadas las necesidades de información, el siguiente paso es diseñar un plan de obtención o Collection Management Framework (CMF) que guíe a los equipos de obtención y dé respuesta a esas preguntas. El CMF es un procedimiento en el que se identifican las fuentes de información y se determina la información que se puede obtener de ellas para poder dar respuesta a las necesidades de información del Mando o Dirección (Goss, 2024; Lee et al., 2018).

A modo de ejemplo las necesidades de información a nivel táctico vistos en la anterior tabla podrían traducirse en un CMF como el que se muestra en la Tabla 3-4.

¹⁰ Endpoint Detection and Response. Software que monitoriza y responde a amenazas en dispositivos.

¹¹ Extended Detection and Response. Plataforma que integra y correlaciona datos de múltiples capas de seguridad (endpoints, red, correo electrónico y nube) para detectar y responder a amenazas de forma automática.

	NMAP ¹²	SHODAN ¹³	BURP SUITE ¹⁴	NIST ¹⁵	LEAKS ¹⁶	OSINT
Hosts activos	X	X				
Puertos y servicios	X	X				
Formularios de entrada web			X			
Correos electrónicos					X	X
CVEs		X		X		

Tabla 3-4 CMF para superficie de exposición (elaboración propia)

Los CMF se adaptarán al nivel de información requerida, ya sea externa o interna. En la Tabla 3-5 se puede ver un CMF diseñado para un SOC.

	EDR	SISTEMAS WINDOWS	RED	FIREWALL
Tipo de dato	Alertas consola EDR	LOG de HOST	Flujo de red	Alertas SIEM
Fase Kill Chain	Explotación, Instalación	Explotación, Instalación, Acciones en Objetivo	Reconocimiento interno, Entrega, C2	Reconocimiento externo, Entrega y C2
Formato dato	Muestra de malware	Ficheros y timelines	Captura de paquetes	Flujo de red
Retención de los datos	30 días	30 días	15 días	60 días

Tabla 3-5 CMF de obtención de información interna para un SOC (Goss, 2024)

A continuación, se propone una metodología ordenada que sigue cada una de las fases anteriormente mencionadas y se presentan algunas técnicas que pueden servir de procedimiento o guía para los analistas.

¹² Herramienta de escaneo de puertos.

¹³ Conocido como el buscador del Internet de las Cosas (IoT). Permite encontrar dispositivos conectados a la red, como servidores, cámaras de seguridad, semáforos o sistemas de control industrial.

¹⁴ Herramienta para realizar pruebas de penetración (PENTEST) en aplicaciones Web.

¹⁵ National Institute of Standards and Technology. Agencia del gobierno de los Estados Unidos perteneciente al Departamento de Comercio.

¹⁶ Exposición no autorizada de datos confidenciales (de manera accidental o intencionada) a un público no autorizado.

3.2 Fase de Obtención

3.2.1 Tipología de fuentes para CTI

La información que analiza la CTI proviene de diferentes fuentes que posibilitan caracterizar a los actores amenaza y las campañas activas. Estas fuentes pueden ser (Zafra, 2025):

- **Fuentes internas:** registros (logs), escaneos, tráfico de red (PCAP¹⁷), análisis de malware, honeypots¹⁸, etc.
- **Fuentes externas:** datasets públicos y privados, feeds de amenazas, bases de datos de vulnerabilidades, certificados TLS¹⁹, etc. Véase la Figura 3-7.

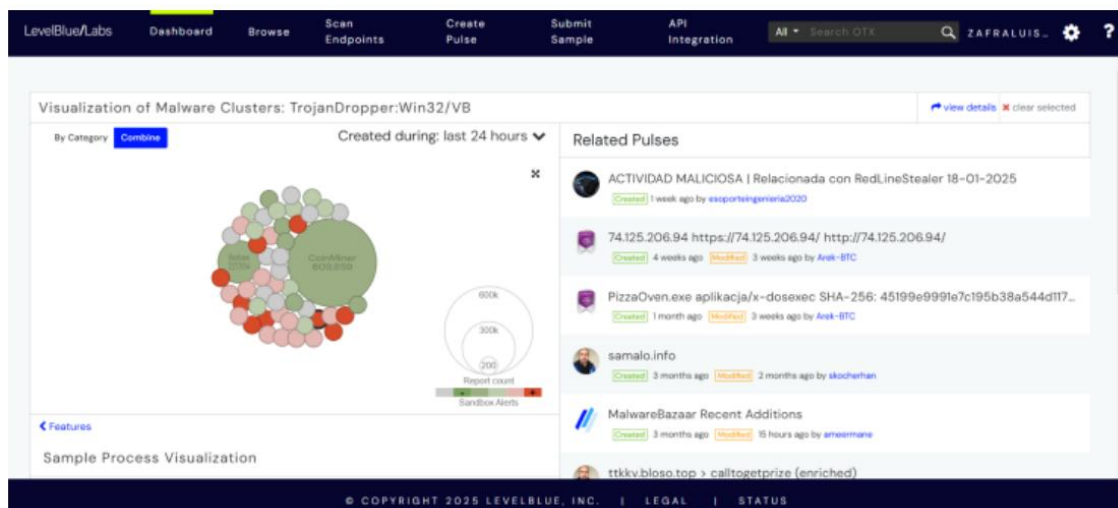


Figura 3-7 Ejemplo del feed de CTI Alien Vault OTX (Zafra, 2025)

3.2.2 Indicadores de compromiso

Un indicador de compromiso (IoC) es una evidencia detectada que indica que la red o sistema ha sido comprometido. Una vez identificado, se debe depurar y validar para evitar falsos positivos. Estos IoC pueden ser de diversos tipos en función de la información que se disponga del ataque, como (Baker, 2025b; Guerra, 2023):

- Hashes.
- Direcciones IP.
- Dominios de Mando y Control.
- Direcciones de correo electrónico.
- URLs.
- Claves de registro.
- Librerías.
- Rutas de fichero.
- Cadenas de texto.

¹⁷ Formato de captura de paquetes de red.

¹⁸ Sistema de señuelo que simula un objetivo de ataque real para atraer a los atacantes sus TTP.

¹⁹ Transport Layer Security. Certificado de seguridad para servidores Web que protege los datos en tránsito entre el cliente (navegador) y el servidor, impidiendo que sean interceptados o modificados.

La generación de IoC conlleva un ciclo (Figura 3-8) que sigue una serie de pasos (SANS Institute, 2009):

- Descubrimiento.
- Análisis.
- Búsqueda y actualización.

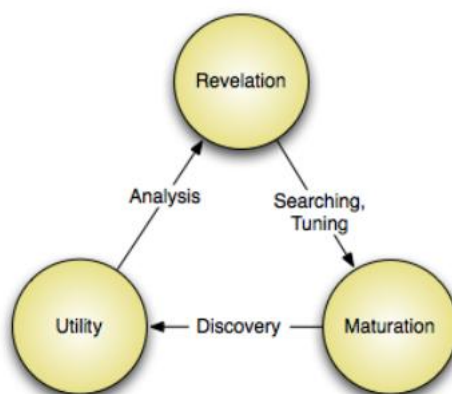


Figura 3-8 Ciclo de vida de un IoC (SANS Institute, 2009)

3.2.3 Pirámide del dolor

Para evaluar la importancia de los IoC obtenidos sirve como referencia el modelo de la pirámide del dolor (Figura 3-9), que clasifica los tipos de IoC según el “dolor” o inconvenientes que un equipo de defensa causa a un adversario al utilizar estos IoC para detectar y bloquear sus acciones. Es decir, que, a mayor dolor o inconveniente para el adversario, mejor defendida estará la red o sistema (Bianco, 2025):

- **Valores de Hash²⁰:** son fácilmente modificables por el atacante. Al tratarse de la firma del malware, una mínima modificación del malware cambiará la firma o hash.
- **Direcciones IP:** una vez bloqueada una dirección IP, el atacante puede cambiar de infraestructura.
- **Dominios:** el atacante deberá adquirir un dominio nuevo y madurarlo para que tenga credibilidad. Ello conlleva tiempo.
- **Artefactos en red o host:** cualquier archivo o rastro dejado por el atacante. Su detección permite al defensor identificar el patrón de comportamiento del adversario y anticiparse a sus próximas acciones.
- **Herramientas:** obligarle al atacante a cambiar de herramientas, puede hacerle desistir de realizar más ataques.
- **TTP:** si se conocen las TTP habituales del atacante, los defensores se anticiparán siempre y dificultarán sus ataques.

²⁰ Algoritmo matemático que convierte los datos en una representación corta y única para garantizar la integridad de la información.

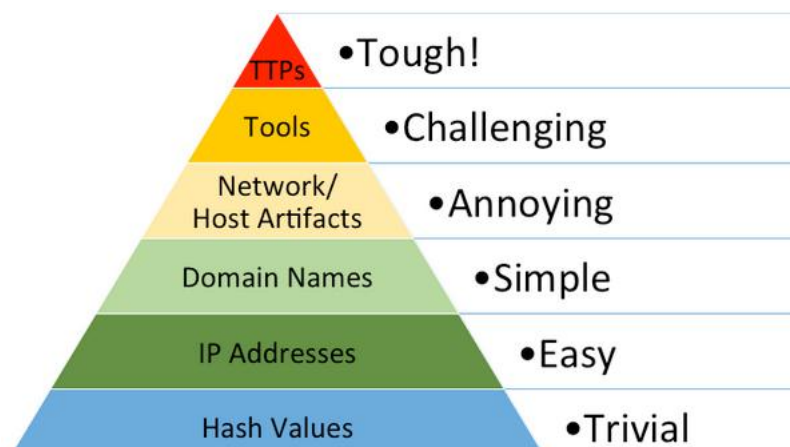


Figura 3-9 Pirámide del dolor (Bianco, 2025)

3.3 Fase de Elaboración

En esta se lleva a cabo el análisis de la información obtenida y la posterior elaboración de productos de inteligencia. Para ello se pueden emplear numerosas técnicas de análisis. A continuación, se propone las técnicas más empleadas en CTI.

3.3.1 Identificación de TTP mediante MITRE ATT&CK

Los actores de amenaza suelen repetir en los ataques sus tácticas, técnicas y procedimientos, así como reutilizar la infraestructura empleada en anteriores ataques con éxito, es decir, sus TTP. Por ello la identificación de las TTP es una acción primordial que debe realizar un analista de CTI (Badger et al., 2016).

- **Tácticas:** Descripción a alto nivel del comportamiento del adversario. P. ej., acceso inicial.
- **Técnicas:** información detallada de la táctica empleada, el camino que ha seguido el atacante o vector de ataque. P. ej., phishing.
- **Procedimientos:** la manera en que el atacante ha desarrollado el ataque. P. ej., correo electrónico con fichero adjunto que tiene una macro maliciosa.

Para estandarizar el proceso y hacer que la inteligencia sea fácilmente interoperable se suele emplear el framework Mitre ATT&CK Enterprise (Figura 3-10). Para facilitar esta labor Mitre proporciona la herramienta Mitre ATT&CK Navigator²¹ (MB Secure, 2019).

²¹ <https://attack.mitre.org/resources/attack-data-and-tools/>

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	27 items	42 items	21 items	57 items	16 items	22 items	15 items	13 items	21 items	9 items	14 items
Supply Chain Compromise	Control Panel Items	Security Support Provider	Access Token Manipulation	Access Token Manipulation	Input Capture	Process Policy	Logon Scripts	Input Capture	Domain Fronting	Data Compressed	Endpoint Denial of Service
Drive-by Compromise	Service Execution	AppCert DLLs	Extra Window	Control Panel Items	Credential Dumping	Score: 5	Pass the Hash	Data from Network Shared Drive	Uncommonly Used Port	Data Encrypted	Network Denial of Service
Spearphishing Attachment	PowerShell	Logon Scripts	Memory Injection	Extra Window Memory Injection	Credentials in Registry	Applicable to: client endpoints	Application Deployment Software	Email Collection	Remote Access Tools	Exfiltration Over Command and Control Channel	Data Encrypted for Impact
Exploit Public-Facing Application	Regsvr32	Image File Execution Options Injection	Process Injection	Masquerading	LLMNR/NBT-NS Poisoning and Relay	Detection score: 4	Distributed Component Object Model	Audio Capture	Commonly Used Port		
External Remote Services	Rundll32	Application Shim	AppCert DLLs	Process Injection	Account Manipulation	System Owner/User Discovery	Exploitation of Remote Services	Automated Collection	Data Obfuscation	Automated Exfiltration	Data Destruction
Hardware Additions	Scheduled Task	Image File Execution Options Injection	Image File Execution Options Injection	Regsvr32	Brute Force	Account Discovery	Clipboard Data	Standard Application Layer Protocol	Exfiltration Over Alternative Protocol	Defacement	Disk Content Wipe
Replication Through Removable Media	User Execution	Scheduled Task	Application Shim	Rundll32	Scripting	System Network Configuration Discovery	Data from Local System	Communication Through Removable Media	Exfiltration Over Other	Disk Structure Wipe	Firmware Corruption
Spearphishing Link	CMSTP	Accessability Features	Application Shim	Image File Execution Options Injection	Exploitation for Credential Access	Application Window Discovery	Remote Desktop Protocol	Connection Proxy			
Spearphishing via Service	Command-Line Interface	Account Manipulation	Application Shim	Image File Execution Options Injection	Forced Authentication	Browser Bookmark Discovery	Remote File Copy	Custom Contr			
Trusted Relationship	Compiled HTML File	Appinit DLLs	Appinit DLLs	Binary Padding	Hooking	Domain Trust Discovery	Remote Services	Data Staged			
Valid Accounts	Dynamic Data Exchange	Authentication Package	Authentication Package	BITS Jobs	Input Prompt	File and Directory Discovery	Replication Through Removable Media	Man in the Browser			
	Execution through API	BITS Jobs	Appinit DLLs	BITS Jobs	Kerberoasting	Network Service Scanning	Screen Capture	Data			
	Module Load	Bootkit	Bypass User Account Control	Bypass User Account Control	Network Sniffing	Network Share Discovery	Shared Webroot	Dom Gene Algor			
	Exploitation for Client Execution	Change Default File Association	DLL Search Order Hijacking	Code Signing	Password Filter DLL	Peripheral Device Discovery	Taint Shared Content	Video Capture			
	Graphical User Interface	Component Firmware	Exploitation for Privilege Escalation	Compile After Delivery	Private Keys						
	InstallUtil			Compiled HTML File							

Figura 3-10 Mapeo de TTP de un atacante según Mitre ATT&CK (MB Secure, 2019)

3.3.2 Cyber Kill Chain

Se trata de un framework creado en el año 2011 por Lockheed Martin que disecciona un ciberataque en siete fases (Figura 3-11). Este enfoque por fases facilita a los defensores el análisis de los ataques y la toma de decisiones. Las fases son las siguientes (Ardal, 2025; Lockheed Martin, s.f.):

- **Reconnaissance:** fase inicial en la que el atacante obtiene información del objetivo.
- **Weaponization:** en la fase de armado se crea el artefacto malicioso o PAYLOAD²² a emplear (malware, exploit, etc.).
- **Delivery:** envío del artefacto malicioso al objetivo.
- **Exploitation:** cuando detona el artefacto y el atacante consigue acceso al objetivo.
- **Installation:** cuando se instala malware o puertas traseras en el objetivo. En esta fase se consigue la persistencia en el objetivo.
- **Command & Control (C2):** conexión del sistema comprometido con la infraestructura del atacante.
- **Actions on Objective:** fase en la que el atacante consigue los efectos deseados del ataque (robo de información, destrucción, etc.).

²² Carga útil de un ataque que contiene el código malicioso. Ejecuta acciones dañinas una vez que se ha explotado una vulnerabilidad.

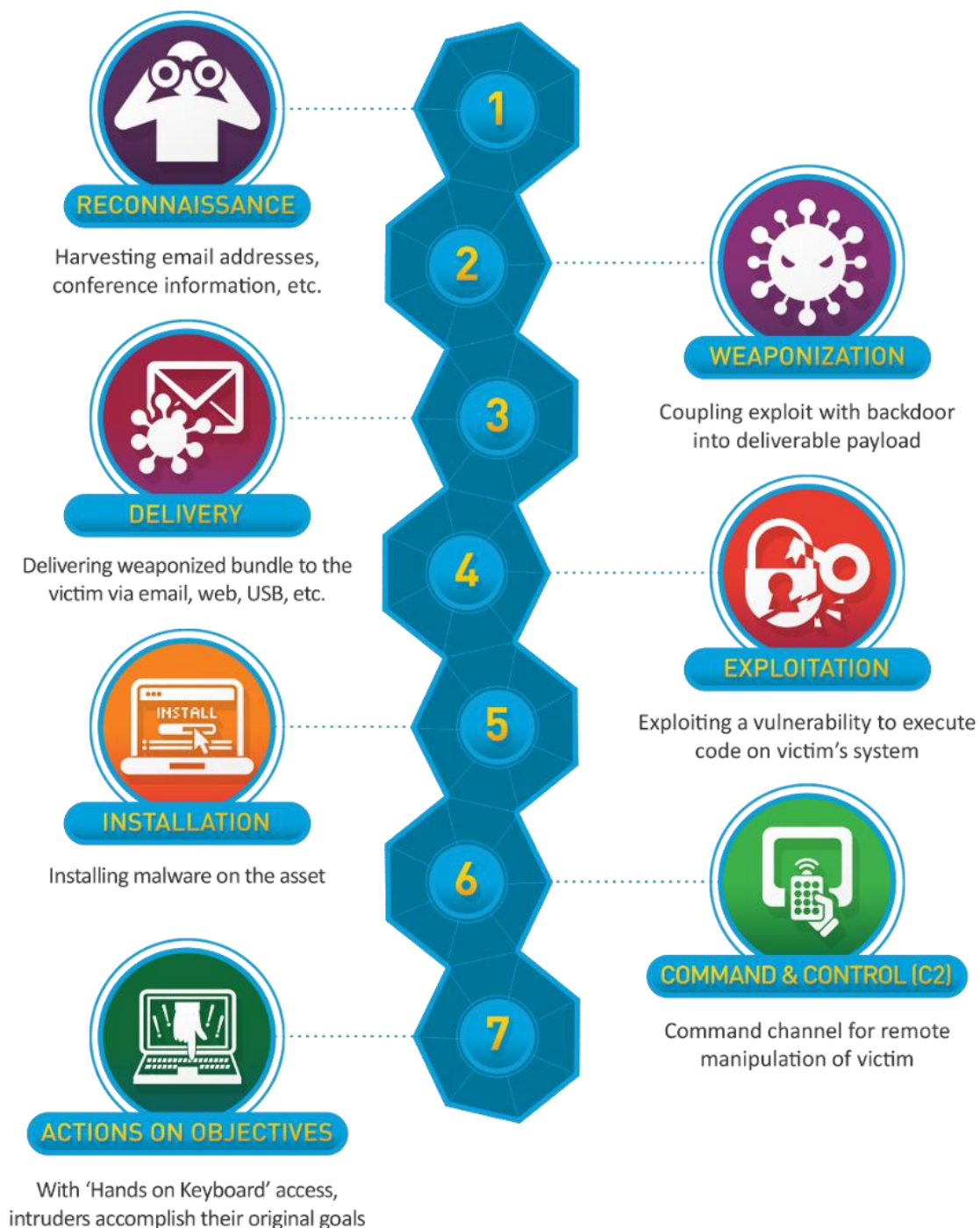


Figura 3-11 Cyber Kill Chain de Lockheed Martin (Lockheed Martin, s.f.)

Para realizar el estudio más claro de un incidente se recomienda combinar la Kill Chain con el framework de Mitre ATT&CK antes visto. De esta manera queda más estandarizado y estructurado con las TTP empleadas por el atacante en cada una de las fases del ataque. Sirva como ejemplo la Tabla 3-6.

FASE	TÁCTICA	TÉCNICA		PROCEDIMIENTO
Reconocimiento				
Preparación	Construcción de capacidades	T1346	Obtención/reutilización de PAYLOADS	Empleo de Cobalt Strike ²³ y PLUGX ²⁴
Distribución	Acceso inicial	T1192	Spear phishing con enlace malicioso	EMAIL temática COVID-19
Explotación	Ejecución	T1204	Ejecución del usuario	Documentos MS WORD con temática COVID. Contienen en su interior ficheros .lnk
		T1106	Ejecución a través de API ²⁵	
		T1059	Interfaz por línea de comandos	
Instalación	Persistencia	T1038	Secuestro de Orden de búsqueda de DLL ²⁶	Ejecución de http_dll.dll para carga del PAYLOAD
	Evasión de Defensas	T1112	Modificación de Registro	
Mando y Control	Mando y Control	T1071	Protocolo Estándar del Nivel de Aplicación	Cobalt Strike. Ocultación del tráfico por medio de peticiones DNS a code.jquery.com. IP C2: 123.51.185.75
Acciones en Objetivo	Evasión de Defensas	T1130	Instalación de certificado raíz	
	Acceso a credenciales	T1081	Credenciales en ficheros	
		T1003	Volcado de credenciales	
	Descubrimiento	T1012	Consulta en el Registro	
		T1082	Descubrimiento de información del sistema	
	Recolección	T1114	Recolección de correos electrónicos	

Tabla 3-6 Perfilado de un ataque combinando Kill Chain y Mitre ATT&CK (elaboración propia)

²³ Herramienta comercial legítima de pruebas de penetración diseñada para emular ataques.

²⁴ Malware de tipo troyano de acceso remoto (RAT).

²⁵ Application Program Interface. Conjunto de reglas y protocolos que permite que diferentes programas de software se comuniquen entre sí, intercambiando datos y funcionalidades.

²⁶ Biblioteca de enlace dinámico. Archivo ejecutable con código y datos reutilizables que pueden ser utilizados por varios programas al mismo tiempo.

3.3.3 Diamond Model

Otra técnica de análisis de ciberataques es el modelo del diamante, que es un framework que estudia los incidentes basándose en cuatro aspectos que, visualizados como los vértices de un diamante, proporcionan a los analistas una síntesis de cómo ha operado el atacante. Los vértices que se analizan son los siguientes (Caltagirone et al., 2013; Tidmarsh, 2023):

- **Adversario:** normalmente no conocido, es el responsable del ataque.
- **Infraestructura:** infraestructura empleada por el atacante (servidores, dominios, etc.).
- **Capacidad:** Tácticas, Técnicas y Procedimientos empleados por el atacante.
- **Víctima:** organización, sistema o red atacada.

En este modelo cada acción o paso que realiza el atacante se denomina evento y conlleva un diamante. La unión de los eventos genera unos hilos de actividad que posibilitan una mejor comprensión de las acciones que ha realizado el atacante (Caltagirone et al., 2013).

La aplicación del modelo del diamante al ejemplo anterior, en concreto a la fase o evento de Mando y Control, quedaría como en la Figura 3-12.



Figura 3-12 Ejemplo de aplicación del modelo del diamante (elaboración propia)

Este modelo se puede combinar con los anteriores para proporcionar una síntesis más clara de los ataques observados, que, como se verá a continuación, posibilitará la aplicación de técnicas de correlación y atribución.

3.3.4 Correlación de eventos

Con los hilos de actividad identificados con el modelo del diamante se puede identificar eventos contra una misma víctima (relacionados verticalmente) y contra varias víctimas (relacionados horizontalmente), dando una primera aproximación a la identificación de campañas o grupos de actividad (Caltagirone et al., 2013). Véase la Figura 3-13.

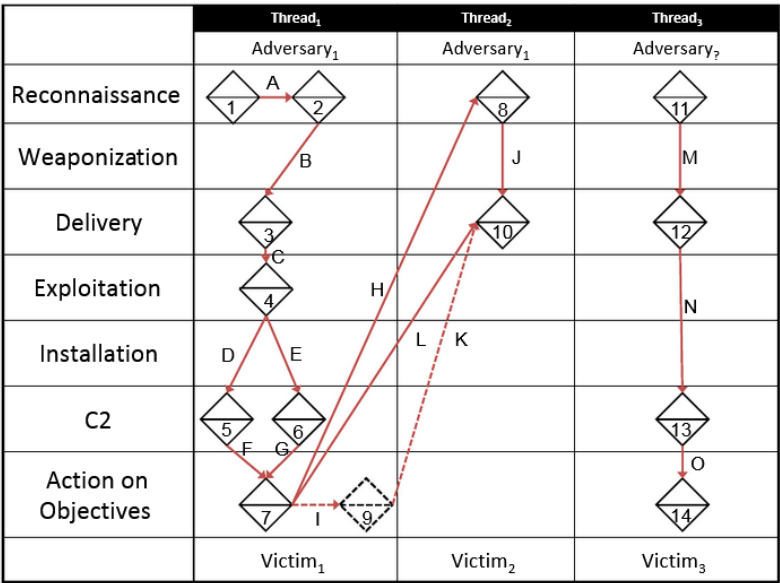


Figura 3-13 Hilos de eventos (Caltagirone et al., 2013)

El conjunto de eventos e hilos de actividad identificados y que guardan correlación por características y comportamientos similares conforman los grupos de actividad (CCN, 2015; Guerra, 2023). Véase la Figura 3-14.

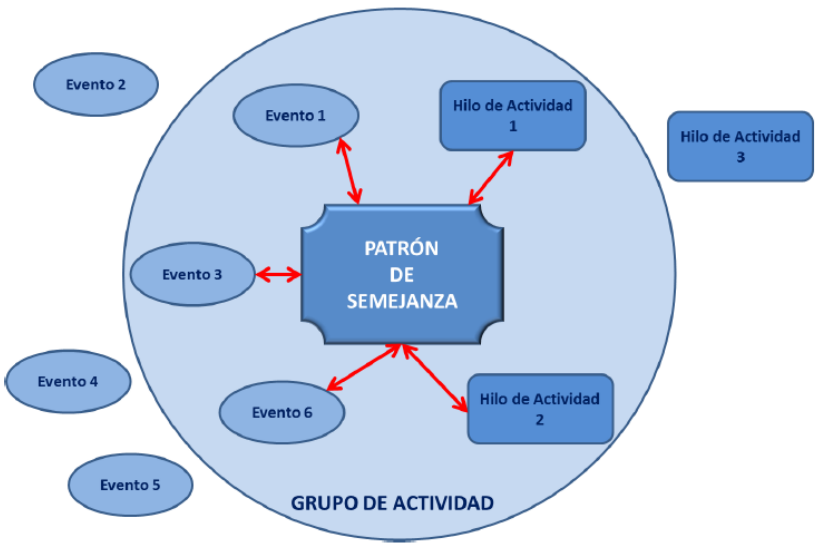


Figura 3-14 Grupo de actividad (CCN, 2015)

3.3.5 Identificación de campañas

Cuando la correlación no es tan clara por falta de evidencia o por la existencia de similitudes entre varios clusters o bien existen discordancias entre los diferentes analistas se emplea el método ACH, que es una técnica para evaluar múltiples hipótesis e identificar la más probable tratando de reducir sesgos. Esta técnica conlleva el seguimiento de una serie de pasos (Sánchez, 2024):

- **Identificación de hipótesis:** Se enumeran las posibles hipótesis candidatas.
- **Enumeración de evidencias:** Se listan las evidencias que se disponen del ataque. P. ej., malware Industroyer, IP maliciosa, etc.

- **Relación de evidencias con las hipótesis:** En una matriz se asocian las evidencias a las posibles hipótesis que apliquen. Se asigna una puntuación con positivos y negativos atendiendo a la probabilidad de cada hipótesis según cada evidencia.
- **Pulido de la matriz:** Se refinan las hipótesis y descartan las evidencias que no aportan valor. Se añaden nuevas hipótesis derivadas del análisis.
- **Evaluación provisional de hipótesis:** Se ordenan las hipótesis en función a su inconsistencia (número de signos negativos).
- **Conclusión final.**

A continuación, en la Tabla 3-8, se muestra el análisis de un supuesto incidente ocurrido en una red. A la vista de los resultados del análisis por ACH, la hipótesis 2 (ciberataque desde el exterior) parece la más probable y la hipótesis 1 (fallo eléctrico) la menos consistente.

	H1	H2	H3
	Fallo eléctrico	Ciberataque desde el exterior	Insider
E1- Información cifrada	-	++	+
E2- Horario nocturno (0517L)	+	+	++
E3- Alerta de evento SIEM (acceso no autorizado)	--	++	+
E4- Muestra de malware	--	++	++
E5- Escaneo agresivo de vulnerabilidades desde el exterior 1 hora antes	--	++	

Tabla 3-7 Evaluación de hipótesis con método ACH (elaboración propia)

3.3.6 Atribución

Una vez perfilado el ataque el siguiente paso es conseguir la atribución. Esta puede ser de varios tipos (Dean, 2024):

- Admisión del adversario. Reivindicación del ataque.
- Publicación de Leaks que incriminen a un autor.
- Acceso directo y detección del atacante. P.ej., entrar en sus sistemas.
- Análisis de la intrusión (atribución técnica).

La parte más importante y difícil para el analista es la de atribución técnica. Se entiende por atribución técnica de la amenaza al conjunto de IoC y TTP que debidamente analizadas en un contexto permiten identificar a los autores de un ciberataque o campaña contra un objetivo (Guerra, 2023).

Según Dean (2024) para que se lleve a cabo un ataque debe haber una intención de llevarlo a cabo, tener la capacidad para realizarlo y una oportunidad para que ocurra el ataque (Figura 3-15).



Figura 3-15 Triada del ataque (Dean, 2024)

Las técnicas de modelado y análisis vistas anteriormente pueden ser empleadas para analizar quién puede estar detrás de un ataque. Por ello, y a modo de recapitulación se propone la siguiente aproximación:

- Tener un conocimiento previo de los actores de amenaza.
- Acudir al modelado e identificación de amenazas realizado en la fase de dirección y planificación. De este ejercicio se obtienen candidatos que puedan atacar a la organización. Estos actores deben tener (Dean, 2024):
 - Intención.
 - Capacidad.
 - Oportunidad.
- Identificación de IoC y TTP.
- Perfilado del ataque según Mitre y Kill Chain.
- Identificación de grupos de actividad con el modelo del diamante.
- Matriz ACH con las hipótesis candidatas y evidencias.

En la Tabla 3-9 se muestra a modo de ejemplo el análisis ACH atendiendo a diferentes actores vistos anteriormente en el ejemplo de modelado de amenazas.

Componente de amenaza	Evidencia	Hipótesis		
		H1	H2	H3
		País XX (motivación anticapitalista, económica)	País YY (motivación espionaje y militar)	Grupo cibercrimen ZZ (motivación económica)
Intención	E4- Tipo de información robada. Estratégica y militar	-	++	-
	E3- Venta de información exfiltrada en foros underground	+	-	++
Oportunidad	E1- Atacante opera en horario de trabajo (0900-1800)	++	++	-
Capacidad	E2- Muestra de malware con caracteres en idioma YY	+	++	+
	E5- Entrada por spear phishing contra personal clave	++	++	+

Tabla 3-8 Ejemplo de Matriz ACH para atribución (elaboración propia)

De un primer análisis, la hipótesis menos consistente es la H3 (grupo del cibercrimen ZZ) y la más probable parece ser la H2 (APT país YY) por tener más evidencias atendiendo a los tres componentes necesarios para la atribución, que son la intención, oportunidad y capacidad. Véase a continuación cómo afectan las evidencias a cada una de las hipótesis:

E1- Atacante opera en horario de trabajo (0900-1800): Es habitual en los grupos APT estatales. H1 y H2 son válidas.

E2- Muestra de malware con caracteres en idioma YY: si bien esta evidencia puede incriminar al país YY, podría tratarse de un ataque de falsa bandera, por ello las tres hipótesis son válidas siendo la H2 la más fuerte.

E3- Venta de información exfiltrada en foros underground: Esta evidencia apunta a la H3, por ser una práctica habitual de los grupos del cibercrimen. No obstante, podría tratarse de la venta en los foros por parte de un grupo cibercriminal pero bajo el encargo del país YY. En este caso se propondría una nueva hipótesis y se volvería a analizar la matriz (pulido de la matriz):

- **H4:** País YY con la colaboración del grupo cibercriminal ZZ para desprestigiar la organización.

E4- Tipo de información robada. Estratégica y militar: esta evidencia se alinea claramente, por su motivación, con H2.

E5- Entrada por spear phishing contra personal clave: El conocimiento del personal clave de una organización suele ser proporcionado por servicios de inteligencia, por ello los grupos APT estatales son candidatos ante esta evidencia (H1 y H2).

Llegados a este punto se obtienen dos hipótesis que apuntan al país YY. Se muestran con su prioridad:

- **(MUY PROBABLE) H4:** País YY con la colaboración del grupo cibercriminal ZZ para desprestigiar la organización.
- **(PROBABLE) H2:** APT País YY.

3.3.7 Mitigación. Matriz de cursos de acción.

Con los modelos de vistos anteriormente, haya atribución o no, el defensor obtiene conocimientos de los incidentes y puede empezar a tomar decisiones de prevención o mitigación. Para ayudar a esta toma de decisiones se puede emplear la matriz de cursos de acción o CoA Matrix, que establece siete tipos de acciones a realizar a cada una de las fases de la Cyber Kill Chain (Amin et al., s.f; Guerra, 2023):

- Detectar.
- Denegar.
- Interrumpir.
- Degradar.
- Engañar.
- Destruir.

Estas siete acciones (7D en inglés) conforman la llamada COA Matrix de Lookeed Martin, que se muestra en la Figura 3-16.

Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance						
Weaponization						
Delivery						
Exploitation						
Installation						
C&C						
Actions on Objectives						

Figura 3-16 Lookeed Martin Course of Actions Matrix (Bahrami et al., 2019)

A continuación, en la Tabla 3-10 se muestra como ejemplo una matriz de cursos de acción con las acciones a realizar ante un ciberataque.

Etapas	Detectar	Denegar	Interrumpir	Degradar	Engañar	Destruir
Reconocimiento	Analítica web	Firewall (bloqueo IP)	Interrumpir acciones de spidering		Publicar direcciones de correo falsas	
Armado						
Envío	Conciencia ción Usuario	Bloqueo de correos	Correos en cuarentena	Particionar ficheros	Redirección de correos sospechosos	Denuncia
Explotación	HIDS ²⁷	Mitigar vulnerabilidad	DEP ²⁸ , ASLR ²⁹			
Instalación	HIDS	Restringir privilegios	Sandbox de aplicaciones			
C2	NIDS ³⁰	Firewall (bloqueo IP)	Vigilar sesiones TCP abiertas (cerrar)	Limitar longitud de sesiones TCP	Honeypot	Contra-ataque, denuncia
Acciones sobre objetivos	Logs (auditoría)	Firewall (bloqueo IP)	Cerrar sesiones TCP en flujos grandes hacia fuera		Honeypot	Contra-ataque, denuncia

Tabla 3-9 Ejemplo de matriz de cursos de acción (Amin et al., s.f.)

3.4 Fase de Difusión

En la última fase del ciclo de inteligencia se comparte la inteligencia elaborada atendiendo al nivel o tipo de inteligencia requerido (Guerra, 2023):

- **Estratégica:** tendencias, perfiles de actores, amenazas emergentes, etc.
- **Operacional:** herramientas, infraestructura, campañas activas, etc.
- **Táctica:** IoC (hashes, IPs, dominios maliciosos).
- **Técnica:** exploits, muestras de malware, vulnerabilidades, etc.

²⁷ Sistema de Detección de Intrusiones basado en host.

²⁸ Data Execution Prevention. Protege frente a la ejecución de código malicioso desde regiones de memoria diseñadas para datos.

²⁹ Address Space Layout Randomization. Técnica que aleatoriza las direcciones de memoria que los programas emplean para dificultar a los atacantes predecir dónde están los elementos críticos para explotar vulnerabilidades.

³⁰ Sistema de Detección de Intrusiones basado en red.

Esta información se comparte con los organismos que se determine en función de su necesidad de conocer (EMAD, 2020). Para ello se establecen mecanismos de clasificación de seguridad o de sensibilidad de la información, así como los protocolos y canales para su distribución, que a continuación se describen.

3.4.1 Sensibilidad de la información

Desde un punto de vista de la inteligencia clásica, un organismo estatal recurrirá a la normativa nacional establecida para clasificar la información. En la Tabla 3-11 se pueden ver los grados de clasificación de seguridad y su equivalente en otros organismos supranacionales.

NACIONAL	OTAN	UE
Secreto	NATO Cosmic Top Secret	UE Top Secret
Reservado	NATO Secret	UE Secret
Confidencial	NATO Confidential	UE Confidential
Difusión limitada	NATO Restricted	UE Restricted

Tabla 3-10 Grados de clasificación de seguridad (CCN, 2012; Hyden, 2025)

Además de los grados de clasificación de seguridad clásicos que se acaban de mostrar, el FIRST creó el protocolo de semáforo o Traffic Light Protocol (TLP) para establecer el modo de proceder para compartir la información clasificada. Este protocolo se basa en el concepto de los semáforos y establece cuatro colores (FIRST, s.f.b), que irán identificados en los productos de inteligencia como se puede observar en el documento de la Figura 3-17.

- **TLP:RED:** sólo puede llegar a destinatarios individuales.
- **TLP:AMBER:** difusión limitada. Se puede compartir la información dentro de la propia organización y/o clientes atendiendo al principio de necesidad de conocer. Si se quiere difundir la información solamente a la organización y no a sus clientes se emplea TLP: AMBER+STRICT.
- **TLP:GREEN:** información restringida a la comunidad. La información no es pública y sólo se puede difundir dentro de la propia comunidad. P. ej., comunidad de ciberseguridad.
- **TLP:CLEAR:** información pública, sin límites.



Figura 3-17 Ejemplo de documento con cabecera TLP:GREEN (Altvater, s.f.)

3.4.2 Estándares de compartición

Desde el punto de vista de la CTI, los IoC y TTP obtenidas en un ataque tienen un ciclo de vida muy corto y deben compartirse de una manera rápida y estructurada para que puedan integrarse de una manera automatizada en las herramientas de los SOC (Pérez & Rego, 2016).

Para ello se muestran algunos de los estándares más empleados actualmente:

- **STIX 2.1:** este estándar denominado Structured Threat Information eXpression consiste en un lenguaje para el intercambio de CTI basado en el formato JSON³¹ (Figura 3-18). Proporciona multitud de objetos para categorizar el tipo de información que se vaya a compartir, algunos de ellos son (Darley et al., 2021; Guerra, 2023):
 - Patrón de ataque.
 - Campaña.
 - Curso de acción.
 - Indicador.
 - Malware.
 - Informe.
 - Vulnerabilidad.
 - Agente de amenaza.
 - Relaciones.

³¹ JavaScript Object Notation. Formato de texto ligero legible por humanos y máquinas para el intercambio de datos. Se basa en una estructura de pares "clave-valor".

```

{
  "type": "indicator",
  "spec_version": "2.1",
  "id": "indicator--f3d3e89c-8f1f-4e93-902c-b9e07b2f42c2",
  "created": "2025-09-17T10:00:00Z",
  "modified": "2025-09-17T10:00:00Z",
  "name": "Dominio de spear-phishing detectado",
  "description": "Dominio usado en campaña de spear-phishing dirigida a personal militar.",
  "pattern": "[domain-name:value='dominio-malisimo.com']",
  "pattern_type": "stix",
  "valid_from": "2025-09-17T10:00:00Z",
  "labels": ["phishing", "malware", "credential-harvesting"],
  "confidence": 75
}

```

Figura 3-18 Ejemplo de reporte STIX 2.1 (elaboración propia)

- **TAXII 2.0:** conocido como Trusted Automated eXchange of Indicator Information, es el protocolo de nivel aplicación que permite transportar información en formato STIX entre sistemas. Está basado en una API RESTful y, como se puede ver en la Figura (3-19), tiene dos modos de compartir la información (Davidson et al., 2017):
 - **Collections:** arquitectura habitual de cliente-servidor. El servidor TAXII dispone de la información CTI en formato STIX y está disponible a los clientes.
 - **Channels:** arquitectura basada en publicador y suscriptores. La información CTI está almacenada en el servidor TAXII y puede ser consultada y actualizada por los suscriptores para luego poderla publicar a otros clientes que estén suscritos a ese servidor TAXII.

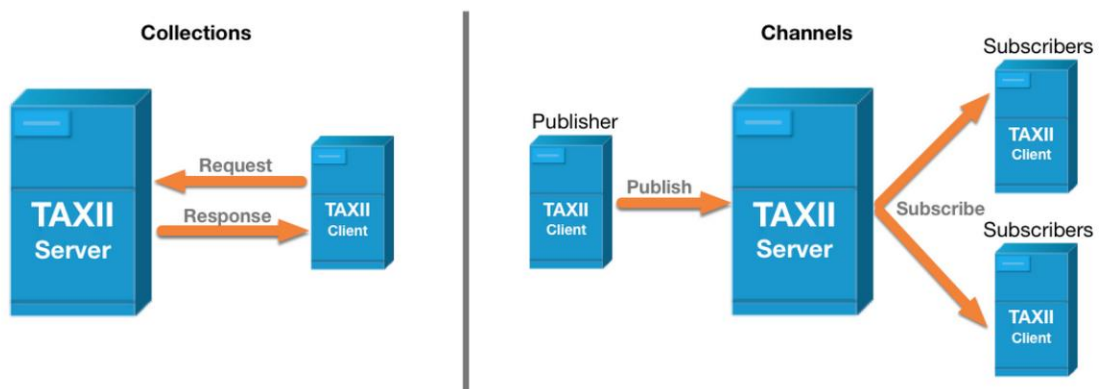


Figura 3-19 Modos de operación de TAXII (Davidson et al., 2017)

3.4.3 Plataformas de compartición

Una vez vistos los principales formatos y protocolos para compartir la inteligencia de ciberamenazas, conviene describir algunas de las principales plataformas de compartición:

- **Malware Information Sharing Platform (MISP):** herramienta de código abierto que permite el intercambio de información de malware y sus IoC (Figura 3-20). Trabaja con información en diferentes formatos, como STIX 2.1. MISP proporciona una base de datos centralizada de eventos de seguridad y permite el intercambio de información de manera automatizada, así como

la interconexión con otros sistemas como los SIEM. Ofrece cuatro modos de distribución de la información (Dulaunoy et al., 2016; Guerra, 2023):

- Exclusivamente para el propio usuario o su organización.
- Limitado únicamente a la comunidad a la que pertenece el usuario u organización.
- Comunidades conectadas a la comunidad a la que pertenece el usuario u organización.
- Disponible para todas las comunidades.

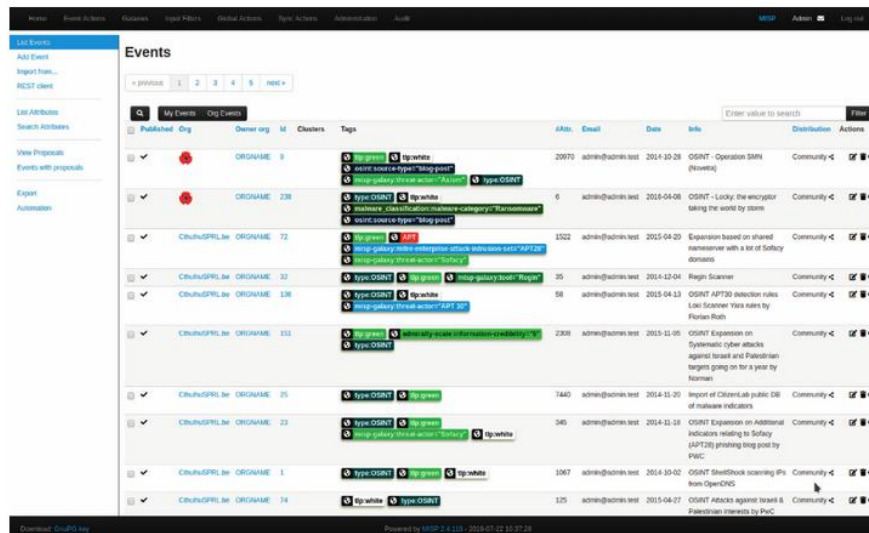


Figura 3-20 Vista de eventos en MISP (Bernabé et al., 2020)

- **The Hive:** es una plataforma de código abierto para la gestión de incidentes de ciberseguridad. Permite la interacción con el MISP así como el trabajo colaborativo entre analistas (IritT, 2024; StrangeBee, s.f.). Véase la Figura 3-21.

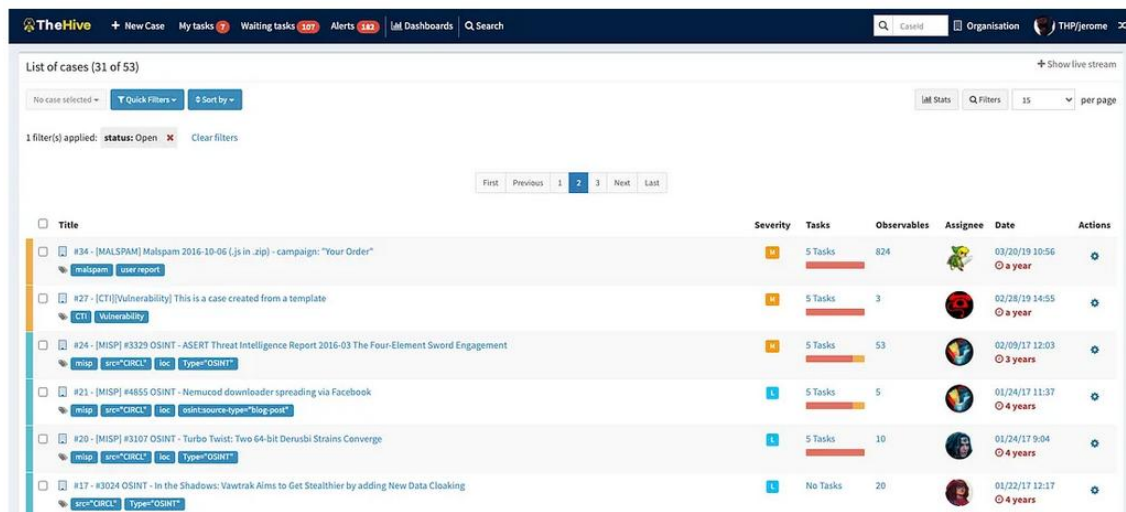


Figura 3-21 Dashboard de la herramienta The Hive (IritT, 2024)

- **OpenCTI:** plataforma de código abierto de gestión y difusión de información sobre ciberamenazas (Figura 3-22). Posibilita el trabajo con información técnica y no técnica y utiliza el formato STIX 2.1 para estructurar la información. Puede integrarse con otras herramientas como el MISP y The Hive (Filigran, s.f.; San José, 2022a).



Figura 3-22 Dashboard de la herramienta OpenCTI (Frayssinet, 2024)

PÁGINA INTENCIONADAMENTE EN BLANCO

4 CIBERVIGILANCIA

La cibervigilancia es una disciplina de la ciberinteligencia que se centra en la monitorización del ciberespacio para identificar de forma preventiva actividades que puedan suponer un riesgo inminente para la propia organización. Se puede considerar como el sistema de alerta temprana en el ciberespacio (S2Grupo, s.f.).

La cibervigilancia vigila todo lo que pueda afectar a la organización en el ciberespacio y las capacidades que suele cubrir varían en función de la naturaleza de la organización o empresa a proteger. Algunas de estas capacidades son (Martin, 2022):

- Identificación de dominios fraudulentos.
- Monitorización de comunidades hacktivistas.
- Identificación de campañas de desinformación.
- Daño reputacional.
- Vigilancia de perfiles falsos de redes sociales.
- Investigación de actores (OSINT).
- Vigilancia de fugas de información corporativa y de credenciales (leaks).

Monitorizar el ciberespacio implica el seguimiento de multitud de fuentes y amenazas en un entorno global, lo cual implica una dificultad enorme para los analistas. Para conseguir una cibervigilancia eficaz y eficiente se necesita seguir un procedimiento ordenado y orientado en este caso a las amenazas en el ciberespacio. Para ello se propone una serie de actividades de monitorización que, a juicio del autor, ayudarán a obtener un sistema inicial de alerta temprana ante amenazas en el ciberespacio.

4.1 Monitorización de dominios fraudulentos

La monitorización de dominios fraudulentos o maliciosos consiste en buscar y alertar del registro de dominios con una denominación y aspecto parecido al de la organización que se protege (Figura 4-1). Estos dominios son utilizados por actores maliciosos para realizar ataques de tipo phishing engañando a las víctimas bajo la apariencia de un dominio legítimo (IT Digital Security, 2023).

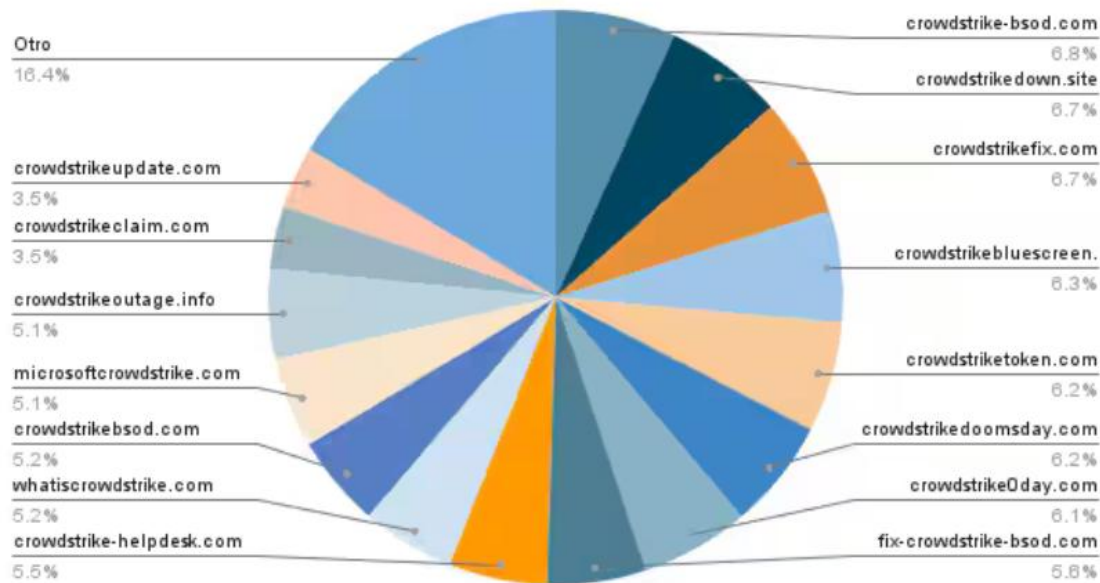


Figura 4-1 Dominios maliciosos asociados a la empresa Crowdstrike (Akamai, 2024)

Los ciberdelincuentes emplean diferentes técnicas para llevar al engaño (Kaminsky, 2023; Tilborghs et al., 2023):

- **Homoglifos:** esta técnica consiste en emplear caracteres visualmente similares con el fin de que el receptor no sea capaz de distinguirlos de los caracteres reales. A continuación, en la Tabla 4-1 y la Figura 4-2 se muestran algunos ejemplos.

CARÁCTER ILEGÍTIMO	CARÁCTER SUPLANTADO	EJEMPLO
l (“L” minúscula)	I (“i” mayúscula)	teIepizza.es
rn (combinación de “r” y “n”)	m	rnicrosoft.com
0 (número cero)	O (“o” mayúscula)	micr0soft.com
ç	c	marca.com

Tabla 4-1 Ejemplos de homoglifos (elaboración propia)



Figura 4-2 Correo malicioso con técnica de homoglifos (elaboración propia)

- **Combosquatting:** consiste en la creación de un dominio que combina su nombre legítimo con una palabra clave. Estas palabras pueden ser del tipo “login”, “admin”, “clientes”, “support”, etc. Sirvan como ejemplo dominios del tipo a los que se muestran en la Tabla 4-2.

DOMINIO ILEGÍTIMO	DOMINIO LEGÍTIMO
banco-clientes.es	clientes.banco.es
mibanco.es	banco.es
login-banco.es	login.banco.es
microsoft-support.com	support.microsoft.com

Tabla 4-2 Ejemplos de combosquatting (elaboración propia)

- **Typosquatting:** esta técnica se basa en escribir mal los dominios de una manera que sea difícil de detectar los fallos. Si alguien lee rápido no se da cuenta de los fallos. En la Tabla 4-3 se muestran algunos ejemplos de dominios fraudulentos empleando esta técnica.

DOMINIO ILEGÍTIMO	DOMINIO LEGÍTIMO
office.com	office.com
gogle.com, gooogle.com	google.com
amazn.com	amazon.com
wikipedia.org	wikipedia.org

Tabla 4-3 Ejemplos de tiposquatting (elaboración propia)

- **TLD Squatting:** consiste en la sustitución del dominio de nivel superior (TLD). De esta manera, al cambiar el dominio TLD el nombre de la empresa suplantada sigue siendo el mismo. Véanse algunos ejemplos en la Tabla 4-4.

DOMINIO ILEGÍTIMO	DOMINIO LEGÍTIMO
amazon.co	amazon.com
office.pro	office.com
bbva.xyz	bbva.es
marca.net	marca.com

Tabla 4-4 Ejemplos de TLD squatting (elaboración propia)

La cibervigilancia monitoriza los registros de DNS³² buscando dominios de nueva creación con las técnicas antes descritas.

4.2 Monitorización de fugas de información

Uno de los ciberataques más comunes es el robo de información de una organización (Figura 4-3). Éste puede afectar a información corporativa, cuentas y credenciales, datos personales, financieros, etc. Cuando el robo de información se realiza de manera intencionada mediante una intrusión sin autorización en un sistema ajeno aprovechándose de una vulnerabilidad se suele categorizar como Data Breach y cuando esta filtración de datos no es intencionada se denomina Data Leak (Portillo, 2019).

³² Domain Name System. Protocolo que convierte nombres de dominio en direcciones IP.

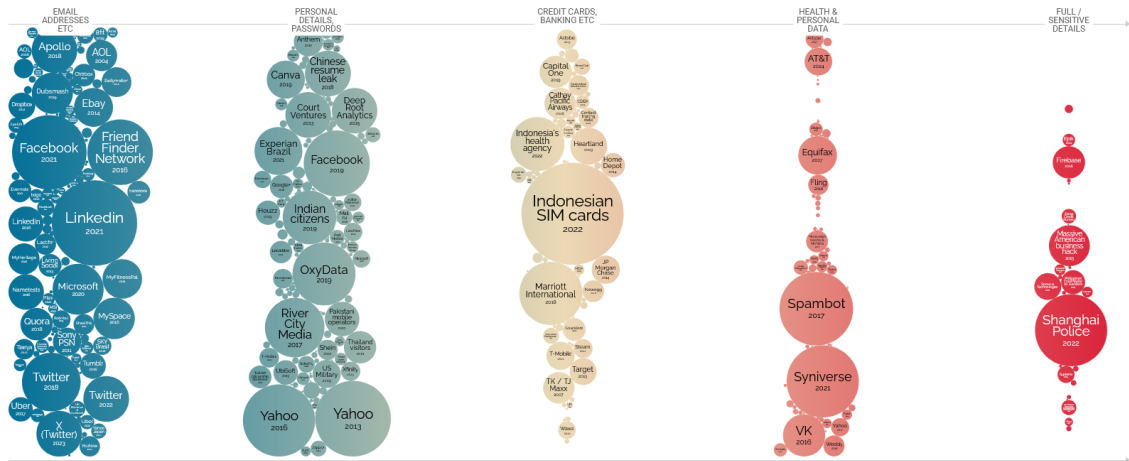


Figura 4-3 Mayores brechas de datos de 2024 clasificadas por tipo (McCandless et al., 2024)

Los leaks se monitorizan en foros clandestinos, mercados negros y canales cerrados de la Dark Web, redes sociales abiertas y cerradas (Darknetsearch, 2025). En la Figura 4-4 se puede observar la publicación y venta de leaks en foros de este tipo.

SQL Drizly.com [2.4M]	Databases	5	415
SQL Omaze.com	Databases	7	1,637
SQL Vakinha.com.br [4.8M]	Databases	1	355
SQL Chatbooks.com [15M] (1 2)	Databases	13	806
SQL Hurb.com [20M] (1 2)	Databases	16	1,641
Promo.com [22M] (1 2)	Databases	15	1,738
SQL BHINNEKA.COM (1 2)	Databases	12	1,804
CSV Mathway.com [25M]	Databases	7	611
CSV Appen.com [5.8M]	Databases	3	597
Swvl.com [4M]	Databases	9	969
EMAIL-PASS LIVEauctioneers [2.943.438] (1 2 3 4 5)	Dehashed Combolists	55	1,422
Wattpad SHA256 w/ Salt (1 2 3)	Databases	30	2,852

Figura 4-4 Publicación en foro de información robada (Abrams, 2020)

4.3 Hacktivismo

El término hacktivismo viene de la combinación de las palabras hacker y activismo que, como su propio nombre indica, consiste en la realización de acciones maliciosas en el ciberespacio para promover ideas políticas, sociales o religiosas (S2Grupo, 2024; U-Tad, 2023).

El perfil del hacktivista en general suele ser de baja sofisticación técnica y suele tener como motivación (Lisa Institute, s.f.a; U-Tad, 2023):

- Activismo político.
- Lucha contra la censura o libertad de expresión.
- Protestas contra la corrupción gubernamental.
- Lucha contra la represión.
- Apoyo en conflictos armados.
- Ganar prestigio y notoriedad.

Se pueden diferenciar varios perfiles de hacktivistas, entre los que destacan (Lisa Institute, s.f.a):

- Anónimos: forman grupos sin estructura ni liderazgo y que están formados por múltiples hackers que se unen por una causa en común.
- Ejércitos cibernéticos: son hackers que trabajan para Estados determinados y que actúan en cierta manera como paramilitares radicalizados.
- Militantes: no son autónomos, dependen del que escribe o aporta el relato.
- Oportunistas: suelen buscar reconocimiento y fama y actúan indiscriminadamente sin tener un objetivo o finalidad claros.

4.3.1 Grupos más destacados

Existen numerosos grupos hacktivistas de diferente ideología, siendo algunos de los más famosos (S2Grupo, 2024):

- **Anonymous:** es el grupo más conocido y dispone de presencia mundial con diferentes subgrupos regionales. Anonymous (Figura 4-5), bajo sus diferentes facciones ha estado muy activo en numerosos conflictos, apoyando, entre otros, a Ucrania, Taiwán e incluso a otros colectivos como Wikileaks (Martínez, 2022).



Figura 4-5 Logotipo del grupo hacktivista Anonymous (Bertriu, 2013)

- **LulzSec:** grupo histórico que operó en los años 2011 y 2012. Sus acciones estaban orientadas a auditar y exponer fallos de seguridad a modo de diversión (Figura 4-6). Sus ataques más famosos fueron contra las compañías Sony y Nintendo (Radware, s.f.).



Figura 4-6 Reivindicación de ciberataque contra la web de la CIA por LulzSec (Benedetti, 2011)

- **NoName057(16)**: grupo que se cree vinculado al Servicio Federal de Seguridad de Rusia (FSB). Muy activo en el conflicto de Ucrania. Este grupo intenta desestabilizar los gobiernos de los países que apoyan a Ucrania. En España ha estado muy activo apoyando a las protestas contra el gobierno y realizando ataques de Denegación de Servicio Distribuidos (DDoS) contra páginas webs gubernamentales (Figura 4-7). En julio del año 2024 la Guardia Civil detuvo en España a tres integrantes de este grupo (INCIBE, 2024; Piña, 2025), y un año después en una operación global de EUROPOL, se dismanteló gran parte de su infraestructura conllevando el arresto de numerosos de sus miembros (EUROPOL, 2025).

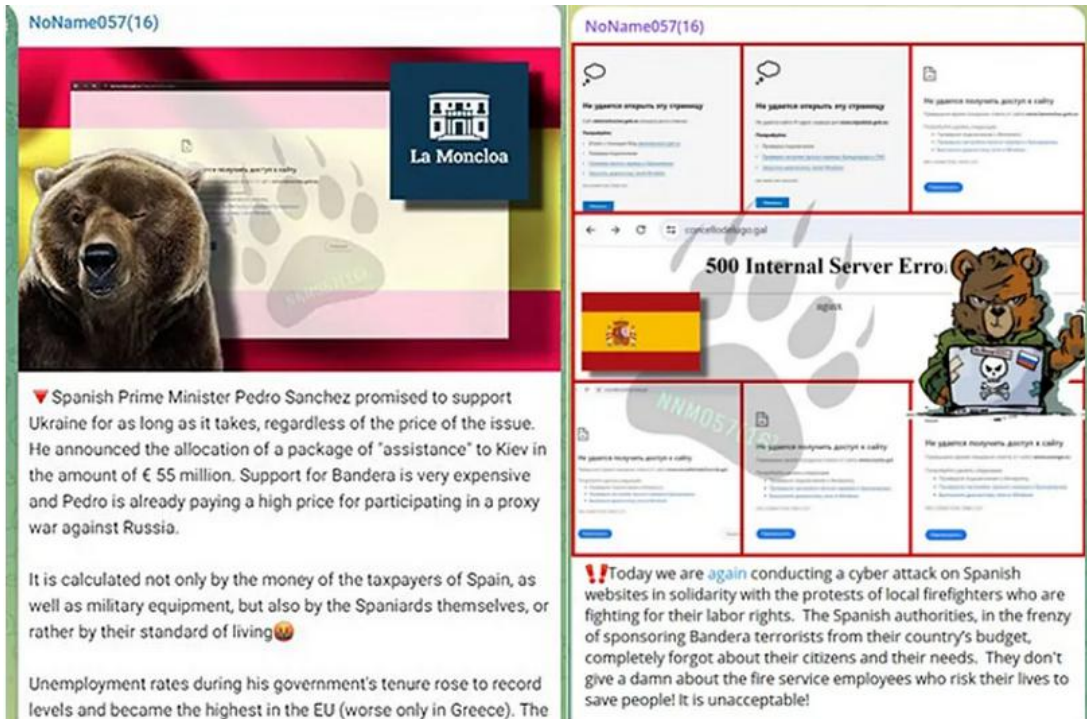


Figura 4-7 Ejemplo de ataque de NoName057(16) contra España (Piña, 2025)

- **Cyber Army of Russia Reborn**: similar a NoName057(16) y activo también en el conflicto de Ucrania. Este grupo (Figura 4-8) se cree de origen estatal y es asociado al grupo APT ruso Sandworm por publicar la información que roba dicho grupo APT (SOCRadar, 2024).

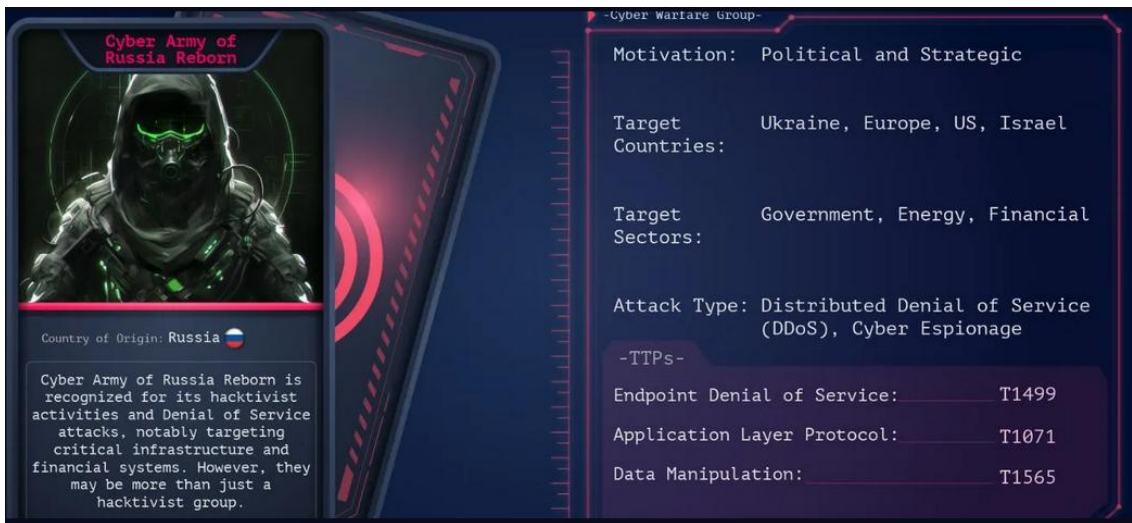


Figura 4-8 Características del grupo hacktivista Cyber Army of Russia Reborn (SOCRadar, 2024)

- **High Society:** se trata de una coalición de grupos hacktivistas prorrusos entre los que se encuentran grupos como Cyber Army of Russia Reborn y 7 October Union. Esta coalición ha realizado ataques contra la OTAN, Europa, Israel, Ucrania y Estados Unidos (Figura 4-9). Entre sus acciones destaca el llamamiento a realizar acciones contra España tras la detención de miembros de NoName057(16) (SC Media, 2024).



We are launching a joint attack with friends from the **Народная Cyber Армия**. They are aimed at the US nuclear and electric power industry. At the moment, two of the largest resources in the field have been disabled. **Nuclear Energy Institute & Electric Power Research Institute**.

Figura 4-9 Anuncio de ataques de High Society contra el sector energético de EEUU (Jain, 2024)

4.3.2 Ataques más comunes

Los tipos de ciberataque más empleados por los grupos hacktivistas son (S2Grupo, 2024):

- Denegación de Servicio Distribuida (DDoS).
- Alteración de páginas web (Defacement).
- Exposición de información personal sobre personas o grupos objetivo para realizar acoso (Doxing).
- Filtración de información confidencial o sensible (Leaks).

4.3.3 Monitorización del hacktivismo

Para monitorizar estos grupos los analistas deben realizar un seguimiento de sus canales (Telegram, X, etc.). Si bien es un trabajo laborioso y discreto, existen numerosas soluciones en el mundo empresarial (Figura 4-10) que proporcionan el análisis y seguimiento de esas comunidades hacktivistas (Terkait, 2024).

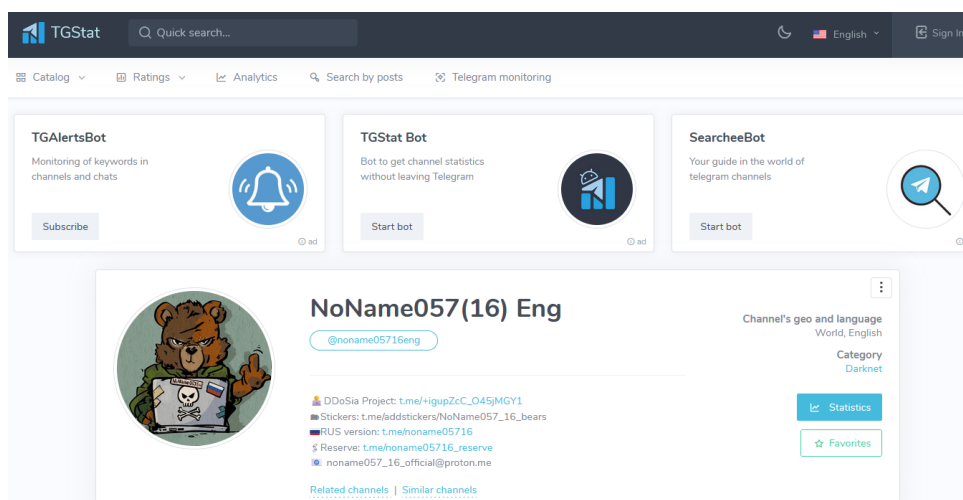


Figura 4-10 Monitorización del canal de Telegram de Noname057(16) (TGStat, s.f.)

4.4 Monitorización de reputación

El control de reputación de marca o de un organismo consiste en realizar un seguimiento de cómo se percibe la organización en Internet (Pinkowska, 2024).

Para ello se monitorizan múltiples fuentes como:

- Redes sociales.
- Foros.
- Podcasts y streaming de video.
- Medios de comunicación.

Los objetivos que se persiguen con esta monitorización, adaptados a las fuerzas armadas son principalmente (Severiche, 2022):

- Gestión de la reputación de marca. En las fuerzas armadas, seguimiento de las acciones STRATCOM³³ (Ruiz, 2024).
- Preparación para posibles crisis o ataques (alerta temprana) contra la organización o contra un evento o cumbre que se esté protegiendo (Méndez, 2022).
- Producción de contenidos adecuados y adaptados para influir en la audiencia objetivo mediante operaciones INFOOPS³⁴ (IEEE, 2020).

4.5 Disciplinas de obtención para cibervigilancia

4.5.1 Inteligencia de Fuentes Abiertas (OSINT)

Open Source Intelligence (OSINT) o Inteligencia de Fuentes Abiertas es una disciplina de la inteligencia que basa su actividad en la recopilación de información a partir de fuentes de dominio público (Martínez, 2014).

Las fuentes de dominio público son numerosas, siendo algunas de ellas las siguientes (Cyber Mentor, s.f.; Lisa Institute, s.f.b):

- Recursos de Internet (portales web, blogs, foros, redes sociales, etc.).
- Medios de comunicación (noticias, radio, televisión).
- Bases de datos públicas.
- Informes y documentos.
- Fotografías, videos y sus metadatos.
- Imágenes geoespaciales (Google earth, imágenes aéreas, etc.).

Las técnicas OSINT se pueden emplear en el marco de una operación CISRO para realizar multitud de acciones, algunas de ellas son las siguientes (Cyber Mentor, s.f.; Martínez, 2014):

- Identificación de posibles amenazas contra la seguridad nacional o en el ámbito militar.
- Realizar auditorías de organismos o empresas objetivo para evaluar su nivel de seguridad y privacidad.

³³ Operaciones de comunicación estratégica.

³⁴ Operaciones de información.

- Evaluar la reputación online de un determinado organismo o empresa objetivo.
- Monitorización del cibercrimen. Obtención de Indicadores de Compromiso (IoC) de campañas maliciosas en el ciberespacio.
- Apoyo a las operaciones militares.
- Apoyo a la investigación de ciberincidentes.
- Apoyo a acciones ofensivas en el ciberespacio (reconocimiento).

Realizar una investigación OSINT conlleva seguir un proceso (Figura 4-11) como el que a continuación se relaciona (Martínez, 2014):

1. Definición de Requisitos. Se determina el alcance de la investigación.
2. Identificación de fuentes de información a emplear y TTP a seguir.
3. Adquisición de la información.
4. Procesamiento de la información.
5. Análisis de la información recopilada y procesada.
6. Elaboración del producto de inteligencia.



Figura 4-11 Proceso OSINT (Martínez, 2014)

4.5.2 Inteligencia en redes sociales (SOCMINT)

La inteligencia en redes sociales o Social Media Intelligence (SOCMINT) es la disciplina de la inteligencia orientada a la recolección y análisis de información obtenida en redes sociales (Goberna, 2025; Lisa Institute, 2023).

El SOCMINT se aplica en diversos ámbitos como en el político, empresarial o en la seguridad nacional (Figura 4-12). Desde el punto de vista de la seguridad nacional, en una operación CISRO el SOCMINT aporta numerosas capacidades, algunas de las cuales se relacionan a continuación (Goberna, 2025):

- Detección temprana de amenazas latentes.
- Prevención de ciberataques.
- Gestión de crisis.
- Mapeo de redes de influencia.

- Identificación de bots.
- Perfilado de grupos e individuos.
- Identificación de operaciones psicológicas encubiertas.
- Identificación de campañas de desinformación.
- Rastreo en tiempo real de actores no estatales.
- Detección de campañas fraudulentas que se viralicen.



Figura 4-12 Aplicaciones estratégicas de SOCMINT (Goberna, 2025)

En el mundo existen numerosas redes sociales y el uso de cada una de ellas depende de la región, costumbres y modas. De todas ellas las más habituales son las siguientes (Martín, 2025a):

- **X (Twitter):** red social y servicio de microblogging orientado al envío de mensajes breves de 280 caracteres como máximo. La mayoría de los usuarios emplean esta red social a través del teléfono móvil, el cual puede proporcionar información valiosa para SOCMINT como la ubicación del terminal (Figura 4-13). Además de la localización, esta red social proporciona a los investigadores información variada como (Bazzell, 2019):
 - Seguimiento de hashtags y tendencias.
 - Búsqueda de usuarios.
 - Análisis de seguidores.
 - Levantamiento de redes de influencia.
 - Búsqueda de usuarios en determinadas zonas geográficas.

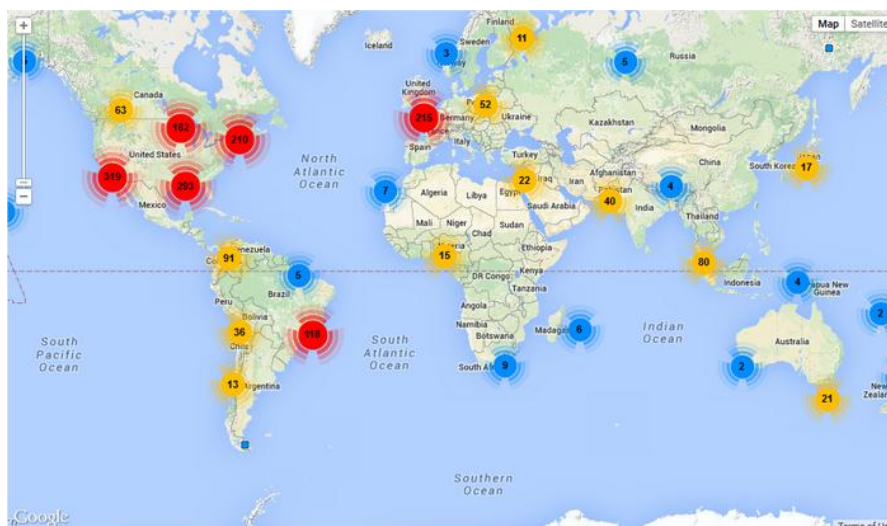


Figura 4-13 Mapeo de localización de seguidores (Lincoln, 2015)

- Facebook:** red social orientada a poner en contacto a personas. Esta red permite a los usuarios compartir información de diferente índole con sus amigos y familiares. La esencia principal de esta red social es conectar usuarios mediante sus gustos y experiencias. La red también permite poner en contacto a personas del mismo sector, ya que sugiere contactos relacionados. Además, permite la creación de grupos temáticos de usuarios que pueden ser abiertos o cerrados. Un investigador puede monitorizar esta red para obtener información de una persona, así como encontrar otros miembros de su comunidad (Figura 4-14) (Regalado, s.f.).

Las analíticas de Facebook son útiles para monitorizar las publicaciones proporcionando métricas como visualizaciones de páginas, likes y compartidos (Suárez, 2024), que pueden ser de utilidad para el seguimiento de operaciones INFOOPS y STRATCOM.

Find your Facebook ID

To find your Facebook personal numeric ID for fb:admins, social plugins, and more, enter your **Facebook personal profile URL** below:

<https://www.facebook.com/YourProfileName>

Find numeric ID →

Figura 4-14 Ejemplo de herramienta de investigación de Facebook (CCAS, 2020)

- Instagram:** red social orientada a la compartición de fotografías entre usuarios. Actualmente es muy popular entre el público adolescente (Soto, 2020). Esta red social proporciona información útil para monitorizar un perfil atacable por técnicas de ingeniería social (Laprovittera, 2024). Existen numerosas herramientas para monitorizar esta red social, una de ellas se puede observar en la Figura 4-15

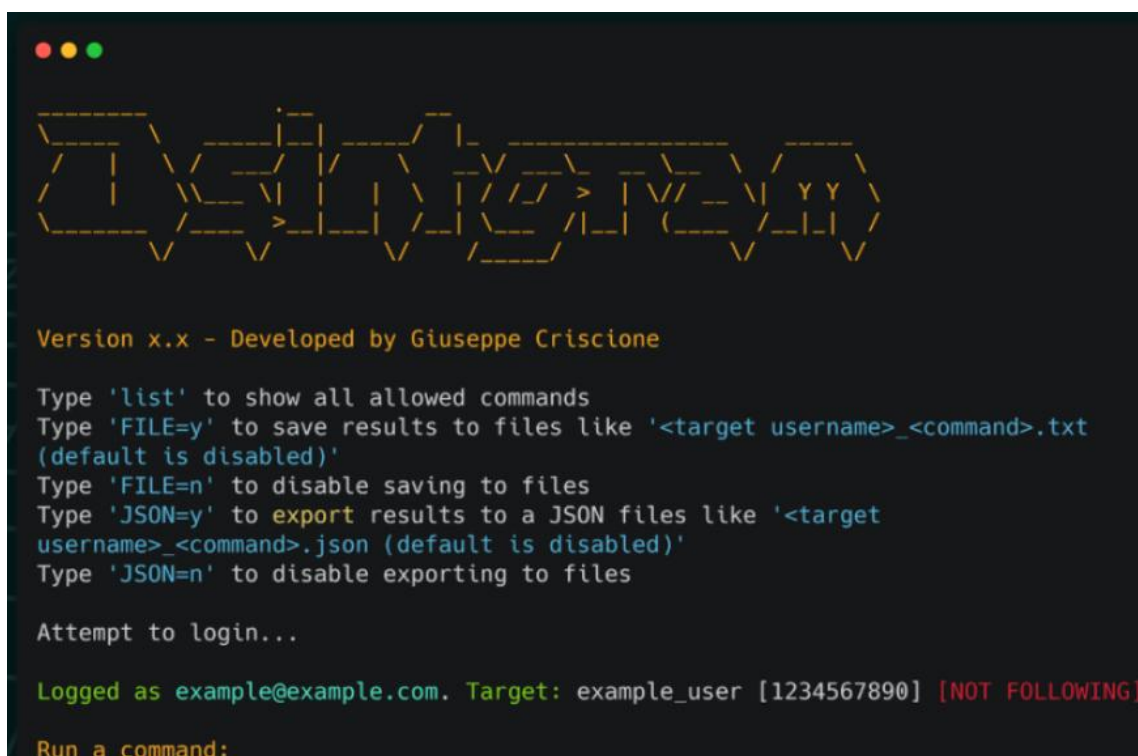


Figura 4-15 Vista de herramienta de OSINT en Instagram (San José, 2022b)

- **LinkedIn:** orientada a relaciones profesionales y comerciales. Esta red permite darse a conocer en el mundo laboral y profesional mediante la publicación de contenidos, videos, debates, etc. (Martín, 2025b). Esta red social es de enorme utilidad para las operaciones CISRO porque permite perfilar los empleados de una organización objetivo. Por ello la monitorización de esta red es una práctica habitual de los servicios de inteligencia (Corera, 2021; Infobae, 2019).
- **Telegram:** red social de mensajería instantánea orientada a la seguridad y privacidad. Ofrece las funcionalidades de mensajes de texto, audio, llamadas de voz y de video, etc. A diferencia de Whatsapp permite la creación de chats secretos, bots y mensajes automáticos, así como la eliminación segura de mensajes. Una de las funcionalidades más interesantes desde el punto de vista de la cibervigilancia es la existencia de grupos y supergrupos privados y públicos (Cibervoluntarios, 2022). Como se ha visto anteriormente en este capítulo, este medio es ampliamente empleado por comunidades hacktivistas así como en el mundo del cibercrimen. Telegram se ha convertido en una fuente imprescindible para los analistas de inteligencia (Arrollo & Volpe, 2025). Además, existen numerosas herramientas y bots para monitorizar Telegram y ayudar en investigaciones (Figura 4-16) (CQCore et al., 2025; Loyalonlytoday, 2025).

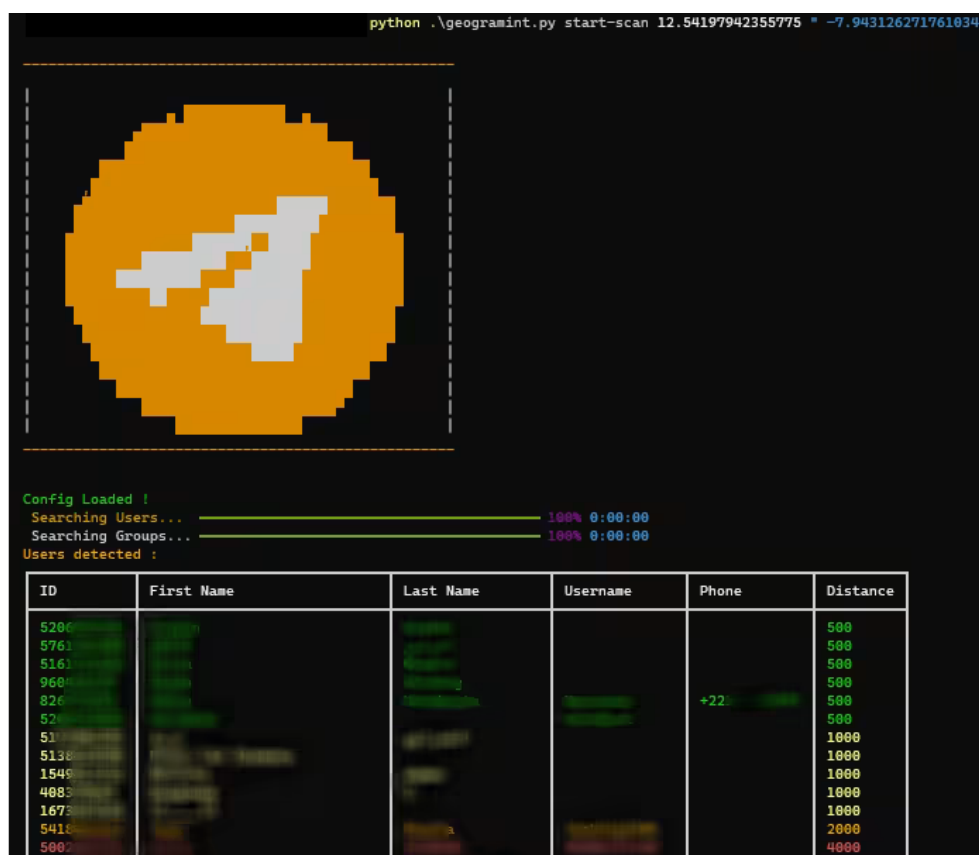


Figura 4-16 Ejemplo de herramienta de geolocalización en Telegram (Esgeeks, s.f.)

- **VK:** con nombre completo VKontakte o ВКонтakte, es el equivalente ruso de Facebook. Esta red social es la más empleada en Rusia y se emplea también en países cercanos como Bielorrusia, Ucrania y Kazajistán. La principal funcionalidad que le diferencia de Facebook es la posibilidad de subir ficheros de audio, escuchar música y ver películas gratis (Taysir, 2021; Véliz, 2021). De cara a su monitorización existen también numerosas herramientas y técnicas OSINT (Bederov, 2022; OSINT Industries, 2025; Rawrdcore, s.f.).

Una práctica maliciosa habitual en redes sociales es la creación de bots³⁵. Normalmente estos bots suelen tener fines de desinformación, tratando de imitar una cuenta legítima para conseguir la confianza de los usuarios y hacerles llegar su narrativa. Los bots se pueden clasificar en varios tipos (Jiménez, 2025):

- **Bots de interacción:** interactúan con los usuarios y pueden tener fines maliciosos como engaño o manipulación.
- **Bots de seguimiento:** siguen a ciertas cuentas de redes sociales con el fin de aumentar el número de seguidores.
- **Bots de difusión de contenido:** comparten contenido de manera automática.
- **Bots de spam:** envían mensajes no deseados. Pueden tener fines maliciosos como phishing o distribución de malware.
- **Bots de falsos influencers:** cuentas falsas que tratan de suplantar a influencers famosos con el fin de conseguir un gran número de seguidores para manipular la opinión de los usuarios y obtener beneficios económicos.

³⁵ Software automatizado que realiza tareas repetitivas y que imita el comportamiento humano.

Existen técnicas para detectar estos bots. Un simple vistazo al perfil puede aportar información útil de cara a su identificación (Figura 4-17), como p. ej. (Jiménez, 2025):

- Única imagen de perfil.
- Nombre de usuario extraño con caracteres raros o muchos números. véase el apartado anterior de homoglifos, combosquatting y typosquatting.
- Carencia de información general de la cuenta.
- Numerosos mensajes repetitivos sobre una misma temática.
- Reciente fecha de creación de la cuenta.
- Ver si responde o no a los comentarios de otros usuarios.
- El perfil no tiene actividad ni seguidores.

En la actualidad se está trabajando en técnicas de identificación de perfiles falsos y bots en redes sociales mediante inteligencia artificial y técnicas de procesamiento del lenguaje natural. (Rigall, 2024).

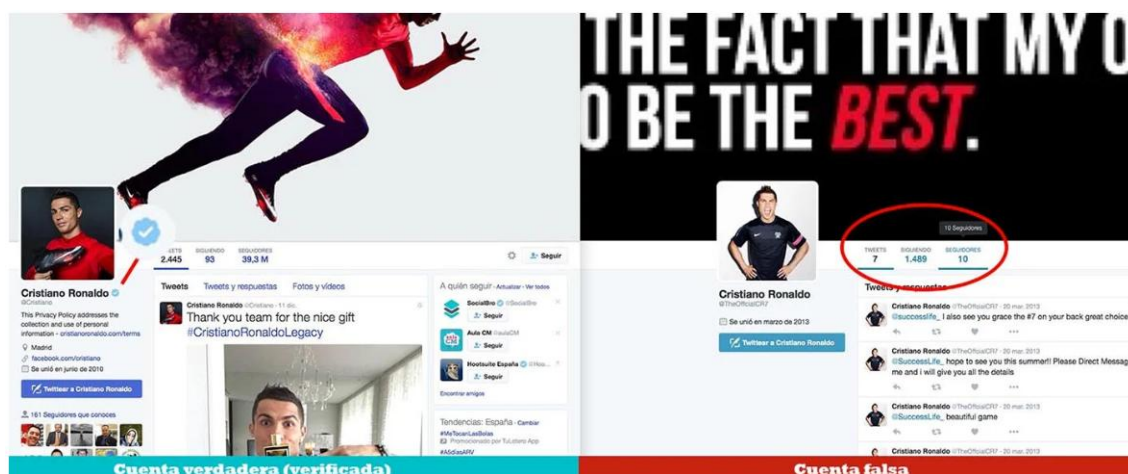


Figura 4-17 Comparativa de cuenta real y falsa en X de Cristiano Ronaldo (OKDiario, 2015)

4.5.3 Virtual HUMINT (VHUMINT)

Según IUCPOL (2023), la Inteligencia de Fuentes Humanas (HUMINT) es la disciplina de la inteligencia encargada de obtener información mediante fuentes humanas.

Análogamente a esta definición, se podría decir que la Virtual HUMINT (VHUMINT) o Cyber HUMINT realiza la misma función que HUMINT, pero obteniendo la información en el ámbito virtual (Seisdedos, 2023).

Desde el punto de vista de la cibervigilancia, las actividades de VHUMINT se orientan a la infiltración en foros y la interacción con usuarios para obtener información. Se trata de un enfoque proactivo de obtención de inteligencia para detectar señales e indicadores previos a los ataques (DeBolt, 2023).

Si bien con el enfoque de OSINT o SOCMINT se puede estar igualmente monitorizando foros, esta actividad se realiza normalmente de una manera automatizada. La información obtenida es valiosa de cara a la alerta inicial de una posible amenaza, pero con VHUMINT se obtiene un poco más pudiéndose comprobar la veracidad de la información publicada en los foros (Tabla 4-5). Esto es posible debido a la infiltración en los canales objetivo habiéndose ganado la confianza de los miembros del foro (DeBolt, 2023).

CASO DE USO	OSINT/SOCMINT	VHUMINT
Riesgo de terceros	Anuncio en foro con descripción genérica de una víctima	Identidad real de la víctima con prueba de validez y evaluación de credibilidad
Gestión de vulnerabilidades	Vulnerabilidad de ejecución remota de código (RCE) revelada recientemente	Un grupo de ransomware planea explotarla para obtener acceso inicial
Amenaza de Insider	Anuncio en un foro que afirma tener acceso privilegiado a un banco	Identidad real del banco y pistas sobre el rol e intención del informante
Gestión de identidad y acceso	Nombre de usuario y contraseña de una víctima de un malware tipo stealer.	Un actor específico de buena reputación en los foros revende las credenciales de administrador de un entorno corporativo
Operaciones de Seguridad de Red (Network Security Operations)	Anuncio de una nueva oferta de malware como servicio	Muestras exclusivas y conocimientos sobre las capacidades y la reputación de desarrolladores y clientes.

Tabla 4-5 Aportación extra de VHUMINT respecto a OSINT y SOCMINT (DeBolt, 2023)

4.6 Redes a monitorizar

Internet está formada por tres capas (Suárez, 2019), todas ellas se emplean como ámbito de actuación en las operaciones CISRO. Véase la Figura 4-18.

- Surface Web.
- Deep Web.
- Dark Web.

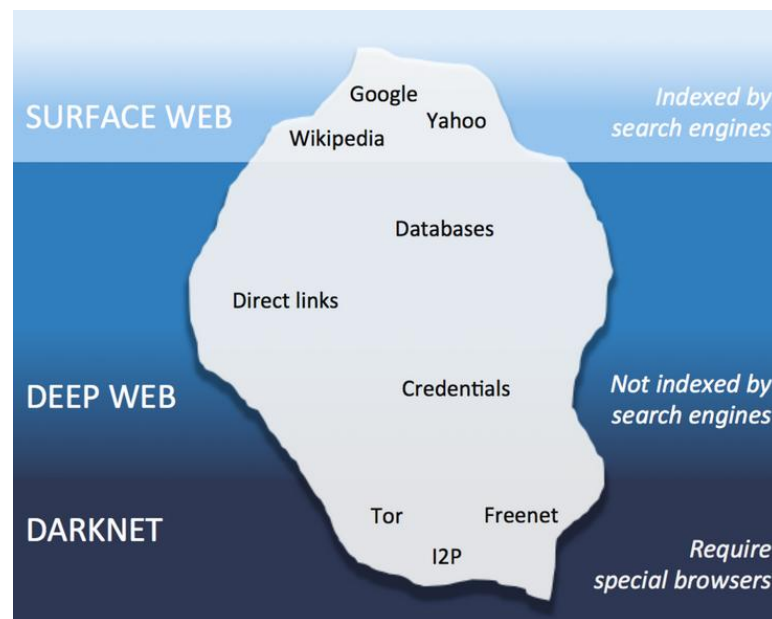


Figura 4-18 Capas que componen Internet (Fernández, 2024)

4.6.1 Surface Web

Es la capa más conocida, visible y accesible. Comprende solamente el 4% de la totalidad de Internet y se puede acceder a ella a través de cualquier navegador y con cualquier buscador. La información está indexada y es accesible desde cualquier dirección IP. En ella se encuentran las páginas web, blogs, redes sociales, etc., y es donde mayoritariamente se realizan las tareas de monitorización con técnicas de OSINT y SOCMINT (Seaton, 2024, s.f.; Suárez, 2019; Voltar, s.f.).

4.6.2 Deep Web

Contiene la información no indexada por los buscadores estándar. Representa aproximadamente el 90% de Internet y suele contener bases de datos privadas, cuentas de correo, servicios basados en suscripción, etc. (Seaton, 2024).

Para acceder a ellas es necesario superar ciertas barreras como suscribirse a un servicio concreto que requiera autenticación y en algunos casos redirigir el tráfico por otros medios como VPN o servidores proxy (Suárez, 2019).

4.6.3 Dark Web

Es la capa más oculta y requiere de herramientas y software específico para acceder. A diferencia de las Surface y Deep Web, la Dark Web está orientada a proveer de anonimato a los usuarios y a los servicios alojados en la red (Seaton, 2024; Suárez, 2019). Esto propicia el desarrollo de actividades ilícitas y por tanto se convierte en un medio a vigilar (Malwarebytes, s.f.).

Existen distintos tipos de redes en la Dark Web:

- **Tor:** red orientada al anonimato y la privacidad. Su diseño está basado en un enrutamiento por capas (onion routing) que redirige el tráfico por diferentes capas. La información se cifra con cifrado asimétrico. Primero se cifra con la clave pública del último nodo, luego con el penúltimo nodo y así sucesivamente hasta llegar al nodo inicial. De esta manera se van creando capas a modo de cebolla en las que sólo los nodos de cada ruta pueden descifrar su capa, garantizándose así la confidencialidad de la información (Fernández, 2021; Ghimiray, 2024). Véase la Figura 4-19.

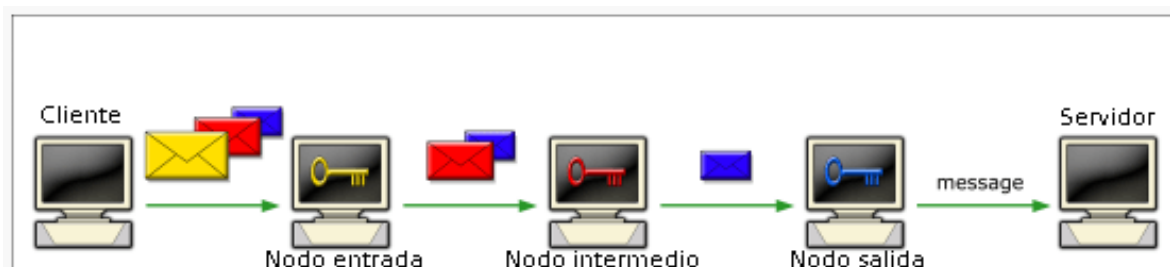


Figura 4-19 Cifrado onion de red Tor con 3 nodos (Carles, 2016)

- **I2P:** red anonimizada descentralizada similar a Tor orientada desde su diseño al anonimato (ciberseguridad, s.f.). La principal característica de esta red es la protección contra la interceptación y análisis de las comunicaciones. Se diferencia de Tor en algunas cuestiones como las siguientes (Jiménez, 2023; Rodríguez, 2017):
 - Usa túneles direccionales diferentes de salida y de entrada, con dos nodos cada uno (Figura 4-20).
 - Envía varios paquetes en una comunicación, Tor envía solo uno.
 - Túneles de vida corta. Dificultan la interceptación por parte de atacantes.
 - Los sitios web son especiales y solo accesibles a usuarios de I2P. Se denominan eepsites.

Por lo general I2P se emplea para acceder a eepsites específicos, no para acceder a la Surface Web (ciberseguridad, s.f.).

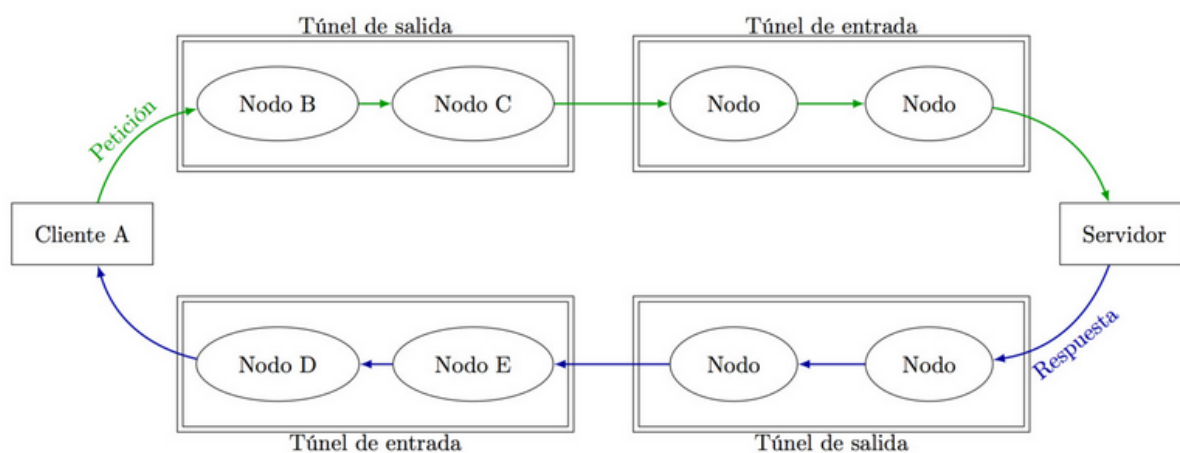


Figura 4-20 Túneles y nodos I2P (Rodríguez, 2017)

- **Freenet:** red descentralizada tipo peer to peer que permite compartir ficheros de manera anónima y el acceso a webs específicas (freesites). La red la forman los usuarios compartiendo parte de sus discos duros y de su ancho de banda. Análogamente a otras Dark Web, protege la información cifrándola a través de nodos (Tannhausser, 2012; Yubal, 2016). Es una red cerrada que no permite alcanzar la Surface Web y que tiene como principal finalidad la privacidad y evitar la censura (Genez, 2020).

PÁGINA INTENCIONADAMENTE EN BLANCO

5 RECONOCIMIENTO

El reconocimiento es la primera fase de una intrusión y comprende las actividades encaminadas a descubrir la mayor cantidad de información posible de un objetivo para poder acceder a él (Astudillo, 2018).

En el marco de la Ciber Kill Chain, el Reconocimiento ocupa la primera de las siete fases que la componen, siendo por tanto una fase crucial de la que dependen las demás. De la información que se obtenga en esta primera fase dependerá el éxito del ataque. Con ella se podrá preparar el artefacto a emplear (Weaponization) así como definir el modo de despliegue del artefacto (Delivery) y las vulnerabilidades a explotar (Exploitation). Dicho de otra manera, la información obtenida proporciona al atacante vectores de ataque de diversa índole como digitales, físicos, de ingeniería social, etc. (Arriols, 2018; Simpère, 2024).

Para llevar a cabo esta fase se debe seguir una metodología ordenada que comprenderá diversas técnicas seleccionadas según el tipo de objetivo al que se enfrente. Se propone al lector aplicar dichas técnicas de forma procedimental y en el orden en que se describen, con el fin de obtener la información del objetivo siguiendo un camino lógico y estructurado.

5.1 Reconocimiento pasivo de infraestructura

El reconocimiento pasivo comprende el conjunto de acciones que no tienen interacción con el objetivo (Astudillo, 2018). Entran en esta categoría la enumeración de DNS, búsqueda de dominios, subdominios, rangos de red y sistemas autónomos (Arriols, 2018).

5.1.1 Búsqueda de dominios del objetivo

En primer lugar, conociendo el nombre de la organización objetivo se busca el dominio principal. Este paso es importante porque la infraestructura expuesta del objetivo depende de alguna manera de este dominio. Es la puerta principal, define el Target y posibilita la información posterior (The Eclipse, 2023).

Una vez obtenido el dominio se suele realizar una búsqueda en la base de datos de los Registros Regionales de Internet (RIR) para obtener datos como el país y ciudad de origen, administrador del dominio, rangos de IP, etc. Existen numerosas herramientas y webs que posibilitan esa información como WHOIS (Figura 5-1), nic.es, etc. (Fernández et al., 2011; Loading, 2024).

```

$ whois uvigo.gal
Domain Name: uvigo.gal
Registry Domain ID: D78-GAL
Registrar WHOIS Server: whois.dinahosting.com
Registrar URL: https://dinahosting.com/
Updated Date: 2022-09-28T07:51:55.502Z
Creation Date: 2014-07-23T15:33:21.706Z
Registry Expiry Date: 2027-07-23T15:33:21.706Z
Registrar Registration Expiration Date:
Registrar: DINAHOSTING S.L.
Registrar IANA ID: 1262
Registrar Abuse Contact Email: abuse-domains@dinahosting.com
Registrar Abuse Contact Phone: +34.981040200
Reseller:
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name:
Registrant Organization: Universidade de Vigo
Registrant Street:
Registrant City:
Registrant State/Province: Pontevedra
Registrant Postal Code:
Registrant Country: ES

```

Figura 5-1 Consulta WHOIS de uvigo.gal (elaboración propia)

WHOIS ha evolucionado al protocolo RDAP, desarrollado por la ICANN³⁶ y orientado a una fácil interpretación por máquinas. Para ello estructura la información en formato JSON (Figura 5-2). Los dos protocolos coexisten actualmente, pero la ICANN está priorizando en su web el uso de RDAP (Álvarez, 2022).

```

"handle": "D78-GAL",
"lang": "latn",
"ldhName": "uvigo.gal",
"links": [
  {
    "href": "https://rdap.nic.gal/rdap/domain/uvigo.gal",
    "rel": "self",
    "type": "application/rdap+json",
    "value": "https://rdap.nic.gal/rdap/domain/uvigo.gal"
  },
  {
    "href": "https://rdap.dinahosting.com/domain/uvigo.gal",
    "rel": "related",
    "type": "application/rdap+json",
    "value": "https://rdap.nic.gal/rdap/domain/uvigo.gal"
  }
],

```

Figura 5-2 Fragmento de información obtenida por RDAP de uvigo.gal (elaboración propia).

5.1.2 Enumeración de DNS

El protocolo DNS, por su diseño, permite realizar una enumeración de este, posibilitando obtener nombres y tipos de registros, direcciones IP, nombres de host, etc. (Bytemind, 2021). Los principales registros DNS se pueden ver en la Tabla 5-1 (Kurose & Ross, 2010).

³⁶ Internet Corporation for Assigned Names and Numbers. Organización internacional que administra y coordina el Sistema de Nombres de Dominio (DNS) y las direcciones IP a nivel global.

TIPO	NOMBRE	FUNCIÓN	EJEMPLO
A	Address Record	Asocia un nombre de dominio a una dirección IPv4	dominio.com IN A 34.147.120.28
AAAA	IPv6 Address Record	Asocia un nombre de dominio a una dirección IPv6	dominio.com IN AAAA 2001:0db8:85a3:0000:0000:8a2e:0370:7334
CNAME	Canonical Name Record	Asigna un alias de un dominio a otro dominio	blog.dominio.com CNAME dominio.com [host] CNAME [dominio destino]
NS	Name Server Record	Especifica los servidores de nombre autorizados para el dominio	dominio.com IN NS ns1.dominio.com
MX	Mail Exchange Record	Indica el servidor de correo para ese dominio	dominio.com IN MX mail.dominio.com
PTR	Pointer Record	Asocia una dirección IP a un nombre de dominio	34.147.120.28.in-addr.arpa IN PTR dominio.com
TXT	Text Record	Posibilita insertar texto en un registro. Por ejemplo, para incluir registros SPF ³⁷ .	v=spf1 ip4:192.168.1.1 ipv4: 192.168.1.25 include:mail.dominio.com -all Autoriza una/s dirección/es IP específica enviar correos a través de los servidores de correo de la organización y rechaza cualquier otro remitente
SOA	Start of Authority Record	Proporciona información varia sobre el dominio como Name Server (NS), administrador, número de serie para las actualizaciones y valores de tiempo (refresh, retry, expire y TTL por defecto)	dominio.com. IN SOA ns1.dominio.com. admin.dominio.com. 2025010701 86400 7200 3600000 3600

³⁷ Registros SPF: autorizan a los servidores de correo electrónico el envío de correos en nombre de un dominio.

DNSKEY	DNS Key Record	Clave pública de los NS que emplean firmas DNSSEC38.	dominio.com IN DNSKEY 256 3 13 <claves_publicas>
DS	Delegation Signer Record	Permite verificar la autenticidad y confianza de las zonas delegadas dentro del sistema de nombres de dominio	Dominio.com IN DS <Número de Clave de Firmante> <Algoritmo> <Tipo de Digest> <Hash>
SRV	Service Record	Indica la localización de un servicio específico en una red, indicando el nombre del host, puerto del servidor, prioridad y peso	_sip._tcp.dominio.com. IN SRV 0 5 5060 sipserver.dominio.com _(servicio)_(protocolo).dominio. IN SRV (prioridad) (peso) (puerto) (host)

Tabla 5-1 Tipos de registros DNS (Kurose & Ross, 2010)

En la Figura 5-3 se muestra a modo de ejemplo parte de la información obtenida del dominio *uvigo.gal* por una web especializada en reconocimiento de DNS.

³⁸ DNSSEC: utiliza firmas digitales para autenticar la integridad y el origen de las respuestas DNS, protegiendo a los usuarios de ataques como spoofing de DNS.

DNS Records for uvigo.gal				
Hostname	Type	TTL	Priority	Content
uvigo.gal	A	0		193.146.32.200
uvigo.gal	NS	0		dns2.uvigo.es
uvigo.gal	NS	0		dns.uvigo.es
uvigo.gal	NS	0		sun.rediris.es
uvigo.gal	NS	0		chico.rediris.es
uvigo.gal	SOA	21600		dns.uvigo.es hostmaster.uvigo.es 2025072201 21600 3600 1814400 21600
uvigo.gal	MX	0	10	mx03.puc.rediris.es
uvigo.gal	MX	0	10	mx04.puc.rediris.es
uvigo.gal	AAAA	0		2001:720:1214:4201::200
www.uvigo.gal	A	0		193.146.32.200
www.uvigo.gal	AAAA	0		2001:720:1214:4201::200

Figura 5-3 Registros DNS de uvigo.gal (elaboración propia)

5.1.3 Enumeración de subdominios

Una vez obtenido el dominio o dominios del objetivo, el siguiente paso es la obtención de subdominios. Para ello se siguen diferentes técnicas como el estudio de DNS antes mencionado, análisis de certificados o técnicas de fuerza bruta (Arriols, 2018).

Desde el punto de vista de un atacante, interesa la resolución de los subdominios para saber así los que están activos y obtener infraestructura para escanear posteriormente. Los atacantes ponen el foco también en los subdominios olvidados, que suelen estar desprotegidos y suelen conllevar múltiples vulnerabilidades (Sharma, 2025). A continuación, siguiendo con el ejemplo anterior del dominio *uvigo.gal*, se enumera en la Tabla 5-2 los subdominios obtenidos asociados a este dominio.

Host	IP	Host	IP
acceso.uvigo.gal	154.59.125.197	lab21.munics.det.uvigo.gal	193.146.32.3
*.acceso.uvigo.gal	154.59.125.197	lab23.munics.det.uvigo.gal	193.146.32.5
autoconfig.alumnado.uvigo.gal	193.146.32.230	lab24.munics.det.uvigo.gal	193.146.32.6
alumni.uvigo.gal	193.146.32.42	lab25.munics.det.uvigo.gal	193.146.32.7
autoconfig.alumnos.uvigo.gal	193.146.32.230	lab3.munics.det.uvigo.gal	193.146.32.13
autoconfig.uvigo.gal	193.146.32.230	lab4.munics.det.uvigo.gal	193.146.32.14
bidi.uvigo.gal	193.146.32.209	lab5.munics.det.uvigo.gal	193.146.32.15
campusactivo.uvigo.gal	193.146.32.205	lab6.munics.det.uvigo.gal	193.146.32.16
celmi.uvigo.gal	193.146.208.187	lab7.munics.det.uvigo.gal	193.146.32.17

ceuvi.uvigo.gal	193.146.32.42	lab8.munics.det.uvigo.gal	193.146.32.18
devtest.cloud.uvigo.gal	193.146.32.244	lab9.munics.det.uvigo.gal	193.146.32.19
conta.uvigo.gal	193.146.32.230	ndn.det.uvigo.gal	193.146.210.3
correoweb.uvigo.gal	193.146.32.224	deypnas01.uvigo.gal	193.146.213.28
dai.uvigo.gal	76.76.21.22	duvi.uvigo.gal	193.146.32.200
eprofun.det.uvigo.gal	193.146.210.15	quiosco.duvi.uvigo.gal	193.146.32.200
lab0.munics.det.uvigo.gal	193.146.32.10	www.duvi.uvigo.gal	193.146.32.200
lab1.munics.det.uvigo.gal	193.146.32.11	ec4rural.uvigo.gal	188.245.36.113
lab10.munics.det.uvigo.gal	193.146.32.20	ecocost.uvigo.gal	82.98.171.200
lab12.munics.det.uvigo.gal	193.146.32.22	ecotox.uvigo.gal	193.146.211.70
lab13.munics.det.uvigo.gal	193.146.32.23	eescoop2025.uvigo.gal	46.231.5.121
lab14.munics.det.uvigo.gal	193.146.32.24	espazos2.uvigo.gal	193.146.32.42
lab15.munics.det.uvigo.gal	193.146.32.25	etdm.uvigo.gal	82.223.107.241
lab16.munics.det.uvigo.gal	193.146.32.26	10 mx04.puc.rediris.es	143.55.148.243
lab17.munics.det.uvigo.gal	193.146.32.27	10 mx03.puc.rediris.es	143.55.146.78
lab18.munics.det.uvigo.gal	193.146.32.28	dns2.uvigo.es	193.146.32.228
lab19.munics.det.uvigo.gal	193.146.32.29	sun.rediris.es	199.184.182.1
lab2.munics.det.uvigo.gal	193.146.32.12	dns.uvigo.es	193.146.32.86
lab20.munics.det.uvigo.gal	193.146.32.30	chico.rediris.es	162.219.54.2

Tabla 5-2 Enumeración de subdominios de uvigo.gal (elaboración propia)

De la información obtenida y mostrada en esta tabla se puede observar los rangos propios de la universidad, la infraestructura alojada en la nube y algunos servicios alojados. Esta información, al igual que la de los siguientes apartados de este epígrafe (5.1) es pública, obtenida de DNS.

5.1.4 Resolución inversa de DNS

Una vez identificados los dominios, subdominios y rangos de red se puede buscar más infraestructura realizando una resolución inversa de DNS. Esta acción se puede realizar de manera pasiva mediante servicios especializados disponibles en Internet o de una manera activa interactuando con los servidores NS (Name Servers) del objetivo, obteniendo así información más completa y fiable (Arriols, 2018). Véase la Figura 5-4.

```

$ nslookup 193.146.36.45
45.36.146.193.in-addr.arpa      name = xcastro.uvigo.es.

Authoritative answers can be found from:

```

Figura 5-4 Ejemplo de resolución inversa por DNS (elaboración propia)

En la imagen anterior, sabiendo que el rango principal de uvigo.gal es 193.146.36.0/24, se ha elegido una dirección IP al azar que no se encontrara en la tabla anterior y, al preguntar a los servidores DNS, se obtiene un subdominio nuevo: xcastro.uvigo.es.

5.1.5 Búsqueda de host virtuales

Con los hosts virtuales, los servidores web pueden alojar varias webs o aplicaciones en el mismo servidor físico. De esta manera se ahorra en recursos y se facilita la administración de los servidores (Slack, 2023).

La organización objetivo puede tener servidores compartidos con otros servicios o aplicaciones, que pueden ser propias o de terceros. Para ello una fase importante del reconocimiento es la búsqueda de host virtuales (Arriols, 2018). En la Tabla 5-3 se pueden observar varios hosts virtuales alojados en un mismo servidor de la Universidad de Vigo.

DIRECCIÓN IP	VHOST
193.146.32.200	duvi.uvigo.gal
	quiosco.duvi.uvigo.gal
	www.duvi.uvigo.gal

Tabla 5-3 Ejemplo de Host virtuales (elaboración propia)

5.2 Reconocimiento activo de infraestructura

De la fase anterior se obtiene bastante información de la infraestructura del objetivo siguiendo técnicas pasivas con una mínima interacción con el objetivo. El siguiente paso es realizar actividades de reconocimiento activo para verificar la información obtenida, así como comprobar los hosts accesibles y los servicios alojados (Arriols, 2018). En esta categoría entran diversas técnicas que a continuación se exponen.

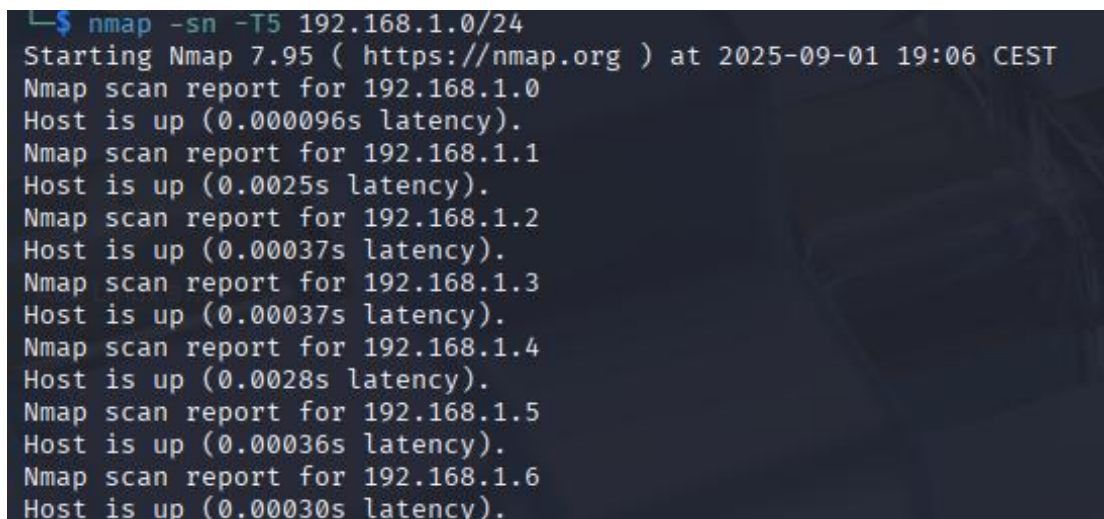
5.2.1 Identificación de host activos

El primer paso de esta fase suele ser la obtención de los hosts activos del rango obtenido en la fase anterior. Para ello existen varias técnicas, algunas de ellas son (Astudillo, 2018; Goss, 2025):

- **Ping Sweep:** se envían peticiones ICMP³⁹ de solicitud de respuesta (echo request) a un rango de IP, y los hosts que responden se consideran activos.
- **TCP-Ping:** en algunos casos se bloquea por seguridad las solicitudes ICMP. El barrido TCP⁴⁰ es un método alternativo que establece una conexión a puertos conocidos y cuando recibe respuesta considera ese destino como un host activo. Véase la Figura 5-5.

³⁹ Protocolo de Mensajes de Control de Internet. Se utiliza para enviar información de control y mensajes de error en redes IP.

⁴⁰ Protocolo de la capa de transporte (capa 4 OSI) orientado a conexión.



```
$ nmap -sn -T5 192.168.1.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-01 19:06 CEST
Nmap scan report for 192.168.1.0
Host is up (0.00096s latency).
Nmap scan report for 192.168.1.1
Host is up (0.0025s latency).
Nmap scan report for 192.168.1.2
Host is up (0.00037s latency).
Nmap scan report for 192.168.1.3
Host is up (0.00037s latency).
Nmap scan report for 192.168.1.4
Host is up (0.0028s latency).
Nmap scan report for 192.168.1.5
Host is up (0.00036s latency).
Nmap scan report for 192.168.1.6
Host is up (0.00030s latency).
```

Figura 5-5 Ejemplo de Ping Sweep (elaboración propia)

5.2.2 Escaneo de puertos

Llegados a este punto, ya se dispone de los hosts que están activos. El siguiente paso es realizar el escaneo de puertos para ver cuáles están abiertos. Los puertos son los puntos a través de los cuales se realiza las conexiones de red y se proporcionan los servicios. Dicho de otra manera, los puertos son como las ventanas o puertas de acceso y desde el punto de vista de un atacante, interesa saber cuáles están abiertas o entreabiertas (Fernández et al., 2011).

Los puertos pueden encontrarse en diversos estados que se muestran a continuación (Astudillo, 2018; Fyodor, 2008):

- **Abierto:** disponible y escuchando posibles conexiones hacia el servicio asociado a ese puerto.
- **Cerrado:** caso contrario del anterior. No dispone de servicios o aplicaciones asociados a ese puerto.
- **Filtrado:** puerto no accesible por la existencia de un dispositivo firewall que impide saber si se encuentra abierto o cerrado.
- **No-filtrado:** puerto accesible pero que no se puede determinar si está abierto o cerrado.
- **Abierto | Filtrado:** estado ambiguo en el que el escáner de puertos no puede determinar si se encuentra abierto o filtrado porque no se recibe respuesta alguna. El puerto puede estar abierto, pero no existe confirmación de ello.
- **Cerrado | Filtrado:** cuando no se puede determinar si el puerto está cerrado o filtrado. Es similar al anterior, pero con el matiz de que el host responde, pero de manera ambigua. Es probable que el puerto esté cerrado y que un firewall oculte esa información.

Las técnicas de escaneo se basan en el envío de paquetes TCP o UDP⁴¹ y el posterior análisis de la respuesta recibida (Astudillo, 2018; Fernández et al., 2011).

En el escaneo TCP se interpreta la respuesta atendiendo al 3-way handshake⁴² (Goedegebure, 2018). Véase la Figura 5-6.

⁴¹ Protocolo de la capa de transporte (capa 4 OSI) no orientado a conexión.

⁴² Proceso de tres pasos para establecer una conexión TCP fiable entre dos dispositivos (cliente y servidor) antes de que se envíe cualquier dato.

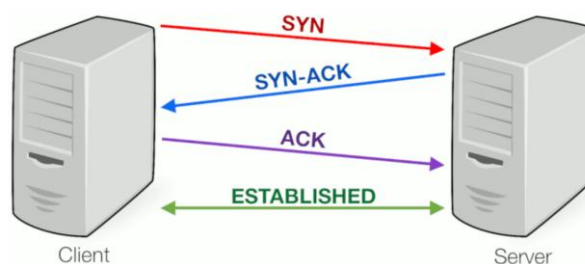


Figura 5-6 TCP 3-way handshake (Goedebure, 2018)

En el escaneo de puertos el análisis de la respuesta TCP recibida nos lleva a la siguiente casuística (Astudillo, 2018; McNab, 2017):

- **Puerto abierto:** el servidor completa el 3-way handshake, se recibe $\text{SYN}^{43} + \text{ACK}^{44}$, como se puede ver en la Figura 5-7.

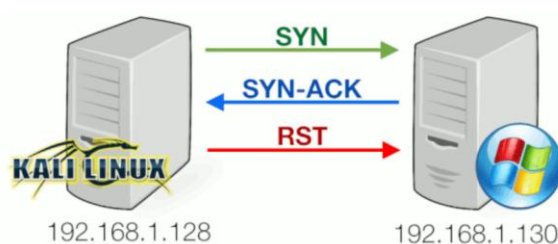


Figura 5-7 Puerto TCP abierto (Goedebure, 2018)

- **Puerto cerrado:** el servidor cierra la conexión, envía un RST^{45} (Figura 5-8).

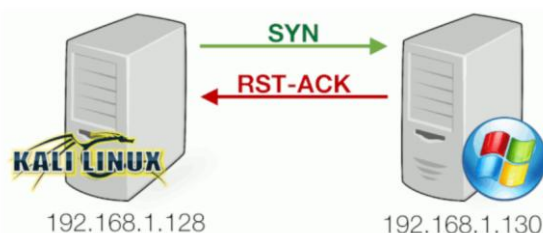


Figura 5-8 Puerto TCP cerrado (Goedebure, 2018)

- **Puerto filtrado:** no se recibe respuesta (Figura 5-9).

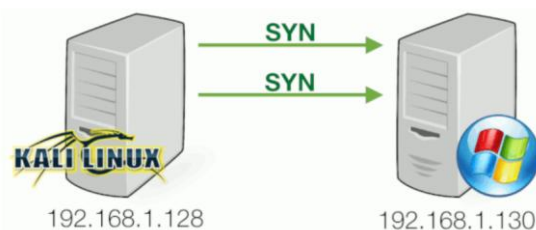


Figura 5-9 Puerto TCP filtrado (Goedebure, 2018)

En el caso de UDP, al tratarse de un protocolo no orientado a conexión, el escaneo es menos preciso. Como se puede observar en la Figura 5-10, se analiza el datagrama UDP atendiendo a la siguiente casuística (Fyodor, 2008):

⁴³ Paquete TCP de sincronización. Establece la conexión inicial.

⁴⁴ Acuse de recibo. Paquete enviado por el receptor para confirmar que ha recibido los datos.

⁴⁵ Paquete que cierra la conexión de manera abrupta.

- **Puerto abierto:** se recibe cualquier respuesta UDP.
- **Puerto cerrado:** se recibe ICMP port unreachable error (type 3, code 3).
- **Puerto filtrado:** se recibe ICMP unreachable errors (type 3, code 1, 2, 9, 10, or 13).
- **Puerto abierto | filtrado:** no se recibe respuesta.

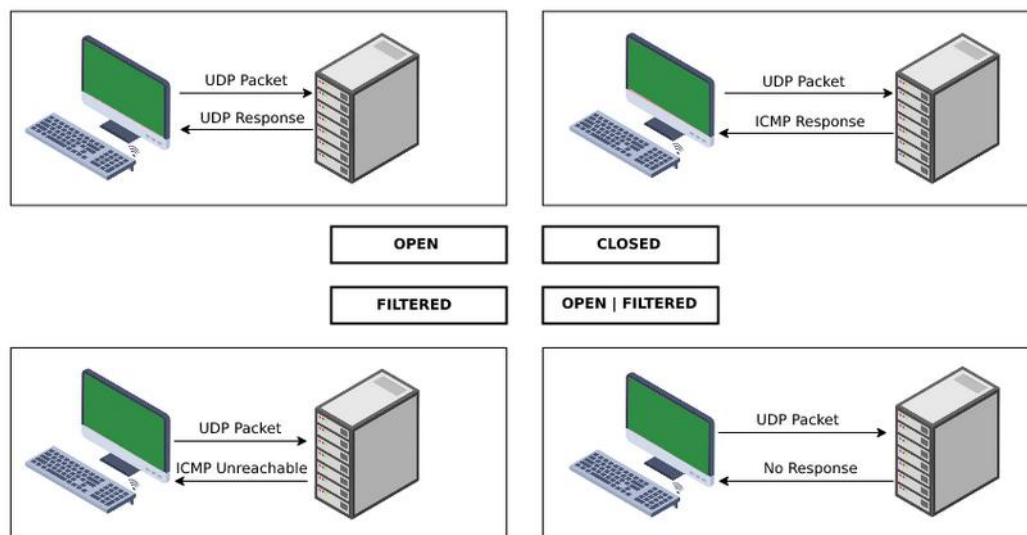


Figura 5-10 Respuestas UDP en escaneo (Geeksforgeeks, 2025)

El escaneo de puertos no solo muestra los puertos abiertos y cerrados de un determinado host o servidor. Se puede ir un paso más obteniendo los servicios alojados tras esos puertos y en algunos casos las versiones de estos servicios. Esta información es muy útil para averiguar vulnerabilidades asociadas a estas versiones. Para ello, la herramienta más conocida es NMAP, que identifica servicios y versiones de estos en función de los datos obtenidos. Las tecnologías o servicios los obtiene de su base de datos interna y las versiones mediante pruebas específicas dedicadas a cada servicio (Figura 5-11). Como se muestra en la Figura 5-12, esta herramienta también propone posibles sistemas operativos que puede tener el objetivo basándose en datos estadísticos y en ciertas pruebas que realiza (Fyodor, 2008).

```

$ nmap -sV scanme.org -T5
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-02 15:42 CEST
Warning: 45.33.32.156 giving up on port because retransmission cap hit (2).
Nmap scan report for scanme.org (45.33.32.156)
Host is up (0.020s latency).
rDNS record for 45.33.32.156: scanme.nmap.org
Not shown: 786 filtered tcp ports (no-response), 210 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http         Apache httpd 2.4.7 ((Ubuntu))
9929/tcp  open  nping-echo   Nping echo
31337/tcp open  tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 42.16 seconds

```

Figura 5-11 Ejemplo de escaneo de servicios y versiones con NMAP (elaboración propia)

```

$ nmap -O scanme.org -T5
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-02 15:45 CEST
Warning: 45.33.32.156 giving up on port because retransmission cap hit (2).
Nmap scan report for scanme.org (45.33.32.156)
Host is up (0.15s latency).
rDNS record for 45.33.32.156: scanme.nmap.org
Not shown: 570 closed tcp ports (reset), 426 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
9929/tcp  open  nping-echo
31337/tcp open  Elite
Aggressive OS guesses: Actiontec MI424WR-GEN3I WAP (96%), DD-WRT v24-sp2 (Linux 2.4.37) (96%), Linux 3.2 (94%), Linux 4.4 (92%), Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012 (92%), Microsoft Windows XP SP3 (90%), VMware Player virtual NAT device (87%), BlueArc Titan 2100 NAS device (86%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 35.38 seconds

```

Figura 5-12 Ejemplo de obtención de Sistema Operativo con NMAP (elaboración propia)

5.2.3 Analizadores de vulnerabilidades

Cuando la discreción no es un requisito el reconocimiento de la infraestructura interna de una organización puede apoyarse en herramientas automatizadas de “botón gordo” (Figura 5-13). Estas herramientas ejecutan de forma agresiva las fases de análisis vistas anteriormente y comparan la información obtenida sobre sistemas operativos, servicios y aplicaciones con una base de datos interna y actualizada de vulnerabilidades (Astudillo, 2018).

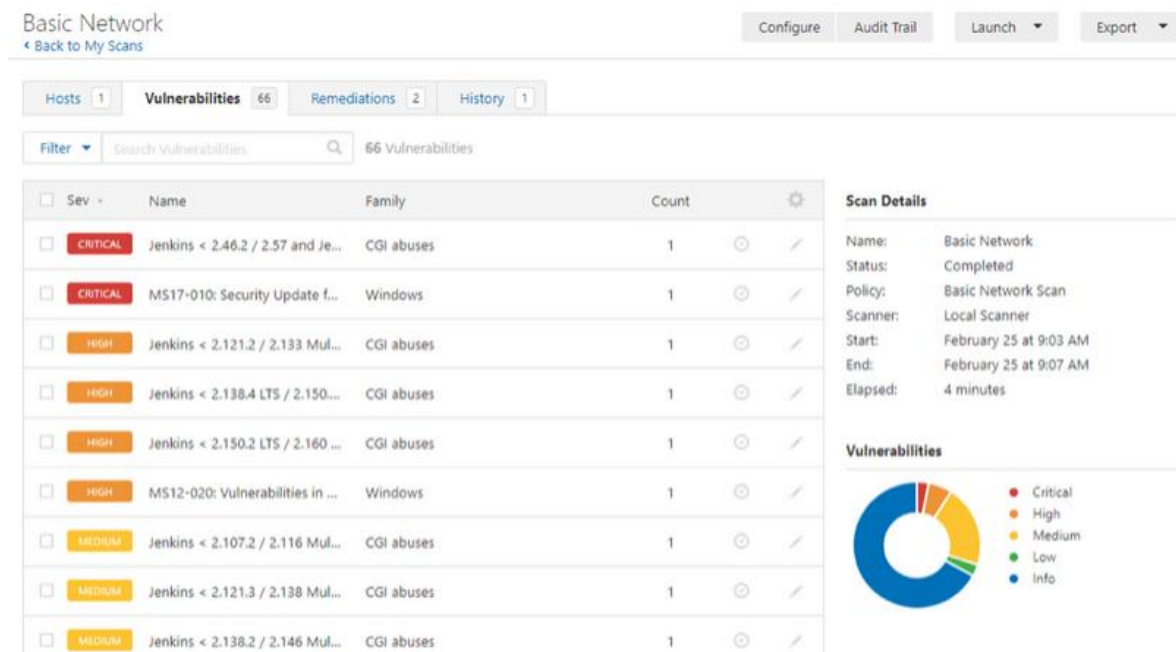


Figura 5-13 Escáner de vulnerabilidades Nessus (Bugcrowd, s.f.)

5.2.4 Fuzzing de aplicaciones WEB

Análogamente a los escáneres de vulnerabilidades se encuentran los fuzzers, que actúan de manera más agresiva e intrusiva contra aplicaciones web. Para ello emplean plantillas con numerosas pruebas de seguridad a realizar con el fin de identificar vulnerabilidades en la web, así como de sortear los

firewalls de nivel de aplicación (WAF). Para ello inyectan infinidad de datos inválidos o inesperados en los formularios de la aplicación web objetivo, detectando así las vulnerabilidades, errores o fallos (Cilleruelo, 2024a).

La herramienta analiza las respuestas a las múltiples peticiones aleatorias en función al código de respuesta HTTP, como se puede ver en la Tabla 5-4 (Pointing, s.f.).

Código HTTP	Mensaje	Descripción
200	OK	Respuesta exitosa
201	Created	Solicitud completada y recurso creado
202	Accepted	Petición aceptada pero todavía no ha finalizado su procesamiento
400	Bad Request	La solicitud está mal formada
401	Unauthorized	Autenticación fallida
403	Forbidden	Autenticación exitosa pero no se tienen permisos para el acceso al recurso solicitado
404	Not Found	No existe el recurso solicitado
405	Method Not Allowed	Método HTTP empleado no permitido
406	Unacceptable	Tipo de contenido no aceptado por la API del servidor
413	Payload too large	La petición excede el límite de tamaño
415	Unsupported Media Type	El tipo de contenido solicitado no es soportado por el servicio
429	Too Many Requests	Petición rechazada por el límite de peticiones (p.ej., ataques DDoS)
500	Internal Server Error	Error inesperado en el servidor debido a la petición
501	Not Implemented	Operación no soportada por el servicio
503	Service Unavailable	Servicio temporalmente no disponible

Tabla 5-4 Códigos HTTP útiles para fuzzing (Pointing, s.f.)

En la Figura 5-14 se muestra un fuzzing para buscar vulnerabilidades del tipo inyección SQL⁴⁶ (SQLi). Para ello se van probando como payload numerosas peticiones. En el momento que el código

⁴⁶ Ataque que aprovecha las vulnerabilidades de una aplicación web para insertar instrucciones SQL maliciosas en los campos de entrada.

HTTP no sea del tipo 200, por ejemplo, uno de la serie 400, será indicativo que el formulario puede ser vulnerable a SQLi.

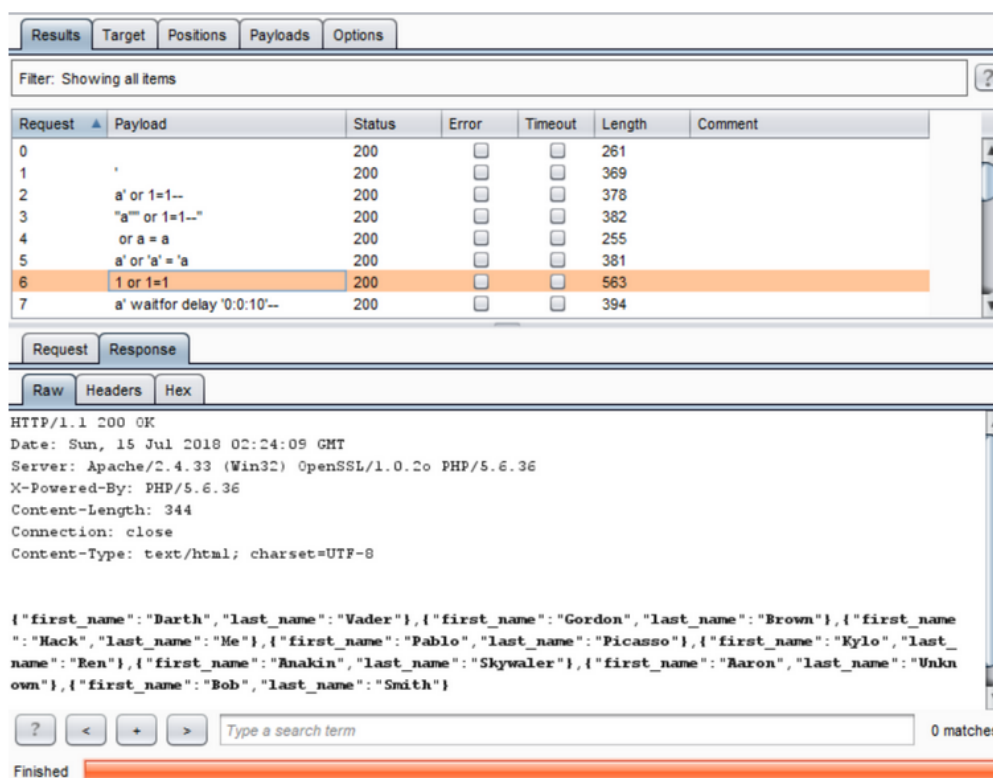


Figura 5-14 Ejemplo de Fuzzing de inyección SQL (Pointing, s.f.)

5.2.5 Análisis de las vulnerabilidades encontradas

Las vulnerabilidades que se identifiquen como resultado del reconocimiento de infraestructura deben categorizarse y reportarse siguiendo un estándar que sea conocido en el mundo de la ciberseguridad, que facilite el intercambio de información entre herramientas y bases de datos, y muestre de una manera clara de qué trata la vulnerabilidad, su peligrosidad y a qué afecta. El estándar más utilizado hoy en día es el CVE (Common Vulnerabilities and Exposures), de la organización MITRE (INCIBE, s.f.).

CVE define una vulnerabilidad como “una debilidad en la lógica computacional (p. ej., código) presente en componentes de software y hardware que, al ser explotada, afecta negativamente la confidencialidad, la integridad o la disponibilidad” (NIST, s.f.).

Las vulnerabilidades se catalogan en la base de datos de CVE con un código CVE único y una breve descripción. La base de datos de los CVE se puede consultar en la web oficial de CVE.org, así como en la National Vulnerability Database (NVD) (Figura 5-15). Además, existen múltiples webs que toman los datos de esta base de datos y que los complementan con otro tipo de información (Enthec, 2024).

El formato de un CVE consiste en CVE-AAAA-NNNNN, donde AAAA corresponde al año en el que se hizo pública la vulnerabilidad y NNNNN al número que se le asigna a la vulnerabilidad (Tripledebleu, 2021).

Identifier	CISA Key Info	Published Date	CNA	Description
CVE-2025-49124	✖	2025-06-16	Apache Software Foundation	Untrusted Search Path vulnerability in Apache Tomcat installer for Windows. During installation, the Tomcat installer for Windows used icacds.exe without specifying a full path. This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.7, from 10.1.0 through 10.1.41, from 9.0.23 through 9.0.105...
CVE-2025-3515	✖	2025-06-17	Wordfence	The Drag and Drop Multiple File Upload for Contact Form 7 plugin for WordPress is vulnerable to arbitrary file uploads due to insufficient file type validation in all versions up to, and including, 1.3.8.9. This makes it possible for unauthenticated attackers to bypass the plugin's blacklist and upl...
CVE-2025-35003	✖	2025-05-26	Apache Software Foundation	Improper Restriction of Operations within the Bounds of a Memory Buffer and Stack-based Buffer Overflow vulnerabilities were discovered in Apache NuttX RTOS Bluetooth Stack (HCI and UART components) that may result in system crash, denial of service, or arbitrary code execution, after receiving mali...

Figura 5-15 CVE mostrados en base de datos de NVD (NIST, s.f.)

Cuando se reporta una vulnerabilidad con CVE se calcula el impacto y severidad de esta atendiendo a una métrica llamada Common Vulnerability Scoring System (CVSS). Esta métrica fue creada por el Forum of Incident Response and Security Teams (FIRST), que va actualizándola, estando recientemente establecida la cuarta versión de la métrica, CVSSv4 (NIST, s.f.; López, 2015), como se puede ver en la Figura 5-16.

CVSS v4.0 Ratings

Severity	Severity Score Range
None*	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

Figura 5-16 Cuantificación de la severidad según NVD (NIST, s.f.)

El CVSS se compone de cuatro grupos de métricas (FIRST, s.f.a), como se puede ver en la Figura 5-17. Estas son las siguientes:

- **Base:** indica la gravedad de la vulnerabilidad según sus características propias y constantes a lo largo del tiempo.
- **Threat:** la métrica de amenaza ajusta la gravedad de la vulnerabilidad atendiendo a factores como la existencia de pruebas de concepto y explotación activa conocida. Una vulnerabilidad se convierte en más peligrosa si existen pruebas de concepto o exploits y se sabe que se están empleando.
- **Environmental:** la métrica ambiental adapta la puntuación a un entorno específico. Atiende a la criticidad del sistema vulnerable y a la existencia o no de mitigaciones.
- **Supplemental:** añaden contexto a la vulnerabilidad con atributos suplementarios.

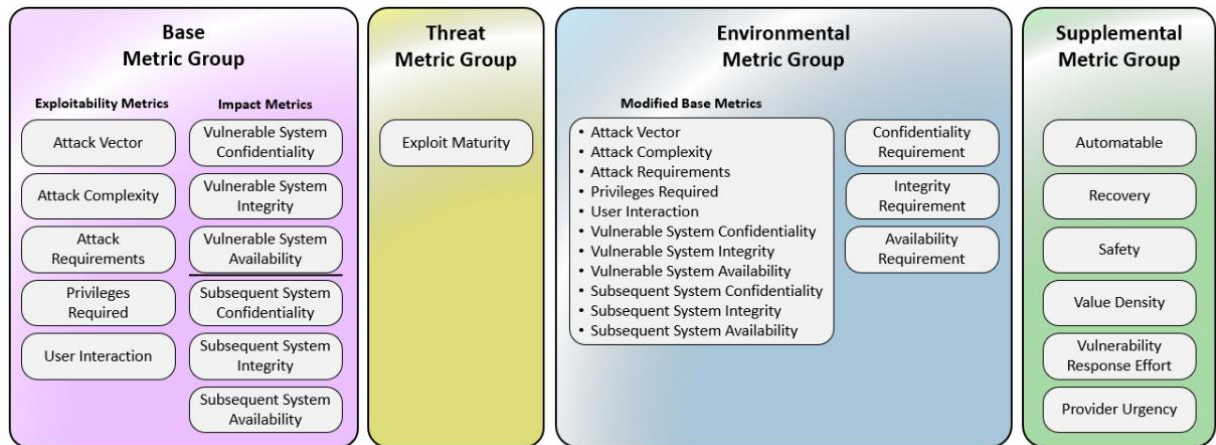


Figura 5-17 Conjuntos de métricas que componen CVSSv4 (FIRST, s.f.a)

Cada grupo de métricas tiene una serie de factores a valorar que generan vectores y estos en su conjunto se combinan en un macrovector resultante con la puntuación obtenida. El NIST proporciona una calculadora (Figura 5-18) que facilita esta labor⁴⁷ (FIRST, s.f.a).

CVSS v4.0 calculator

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:P/VC:L/VI:L/VA:H/SC:N/SI:N/SA:N

CVSS v4.0 Score: 7 / High ⊕

Base Metrics ?

Exploitability Metrics

Attack Vector (AV):

Attack Complexity (AC):

Attack Requirements (AT):

Privileges Required (PR):

User Interaction (UI):

Vulnerable System Impact Metrics

Confidentiality (VC):

Integrity (VI):

Availability (VA):

Figura 5-18 Muestra de la calculadora de CVSSv4 (NIST, s.f.)

En el ejemplo de la ilustración anterior el vector resultante se obtiene de los valores que se han rellenado en la calculadora. P. ej.,

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:P/VC:L/VI:L/VA:H/SC:N/SI:N/SA:N

Siendo los dos primeros valores:

- AV (Attack Vector): N (Network)
- AC (Attack Complexity): L (Low)

⁴⁷ <https://nvd.nist.gov/vuln-metrics/cvss/v4-calculator>

5.3 Reconocimiento de infraestructura inalámbrica

Las redes inalámbricas tipo WiFi pueden suponer un potencial punto de entrada a las redes de la organización objetivo. Estas redes se pueden encontrar con diferentes niveles de seguridad y cifrado (Arriols, 2018):

- **Abiertas:** carecen de medidas de seguridad y cifrado, dejando la información en claro y disponible a cualquiera. Este tipo de redes se suele encontrar como redes de invitados y si no están bien segmentadas pueden suponer un punto de entrada a las redes internas de la organización.
- **WEP:** prácticamente en desuso en la actualidad por haber quedado obsoleto y vulnerable. La información va cifrada por este protocolo.
- **WPA/WPA2 - Personal:** constituyen la evolución de las redes con protocolo WEP, siendo más seguras. Pueden aparecer en algún departamento de la organización.
- **WPA/WPA2 - Enterprise:** redes centralizadas con control de acceso normalmente asociado al dominio interno de la organización. Es el tipo de red que se suele encontrar en las organizaciones.
- **WPA3 -Personal y Enterprise:** versión avanzada y mejorada de los anteriores protocolos. Dispone de un cifrado más robusto y mayor facilidad en la configuración.

5.3.1 Wardriving

Si se tiene la posibilidad de acercarse a las inmediaciones del objetivo se pueden detectar redes inalámbricas tipo WiFi o Bluetooth que pueden suponer un potencial punto de entrada a las redes de la organización. Para ello se emplean técnicas de Wardriving, que consisten en la búsqueda de redes Wi-Fi vulnerables o sin seguridad desde un vehículo. Para ello suelen emplear los siguientes dispositivos (Twingate Team, 2024):

- Dispositivos móviles (ordenadores portátiles, teléfonos móviles, Raspberry Pi, Pineapple, etc.).
- Antenas: antenas omnidireccionales de alta sensibilidad para conseguir capturas a gran distancia.
- Dispositivos GPS: para georreferenciar las redes capturadas.
- Software específico.

5.3.2 Enumeración pasiva

Antes de acercarse físicamente a las instalaciones de la organización objetivo se puede tener una idea inicial de las redes inalámbricas que dispone la organización. Para ello se puede recurrir a portales de Internet especializados que disponen de bases de datos con las redes Wi-Fi detectadas y reportadas por sus usuarios (Arriols, 2018). A continuación, se muestra como ejemplo en la Figura 5-19 la enumeración pasiva de las redes inalámbricas identificadas en el Aeropuerto de Vigo.

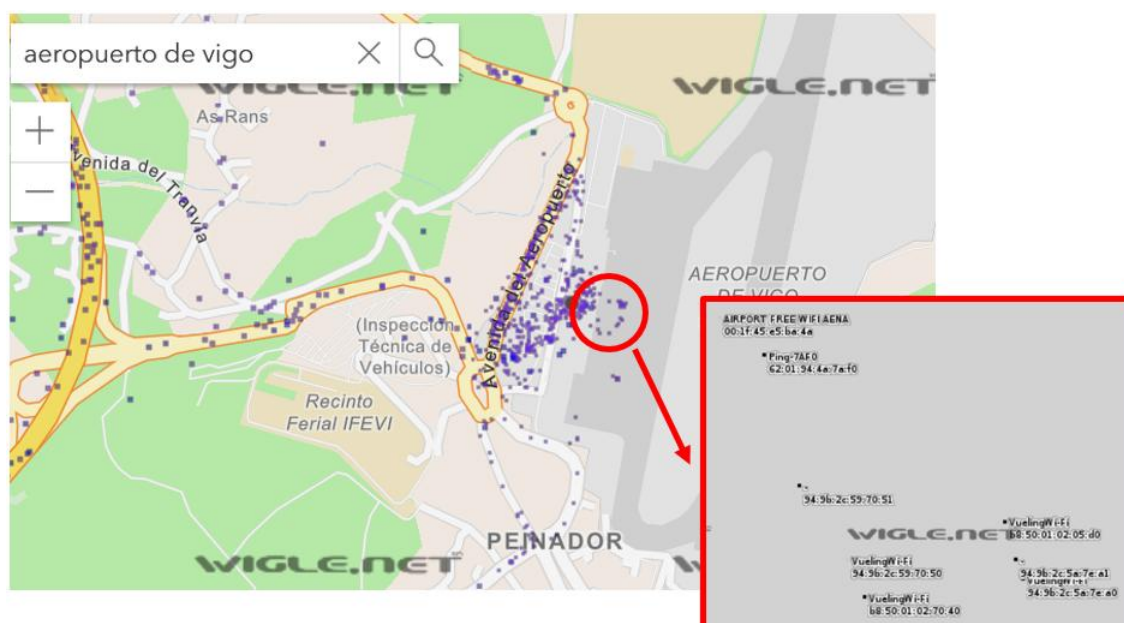


Figura 5-19 Redes Wi-Fi reportadas en el Aeropuerto de Vigo (elaboración propia)

En la imagen se puede observar multitud de redes detectadas (puntos azules). Haciendo un aumento en el edificio de la Terminal se pueden observar redes como:

- AIRPORT FREE WIFI AENA (00:1F:45:E5:BE:4E)
- Vueling Wi-Fi (b8:50:01:02:05:d0)

5.3.3 Enumeración activa

Una vez obtenida de la fase anterior las redes potenciales que puede disponer el objetivo, conviene acercarse y comprobar de una manera activa con los equipos y software adecuados. Normalmente en esta fase se trata de enumerar las redes, el tipo de seguridad y cifrado que emplean, y se captura toda la información que se pueda que puedan dar lugar a posibles vectores de ataque como (Arriols, 2018):

- **Paquetes WEP:** mayor número posible de paquetes WEP para romper el cifrado.
- **Handshake de WPA/WPA2 – Personal:** para tratar de averiguar la contraseña de acceso.
- **SSID⁴⁸ y BSSID⁴⁹:** para realizar ataques de puntos de acceso falsos. Útil en redes WPA/WPA2 – Enterprise.

Existen numerosas herramientas de auditoría de redes inalámbricas que capturan paquetes y permiten realizar los tipos de ataque mencionados. La Figura 5-20 muestra una de ellas.

⁴⁸ Service Set Identifier. Es el nombre de una red Wi-Fi.

⁴⁹ Basic Service Set Identifier. Identificador único (dirección MAC de 48 bits) que identifica el punto de acceso Wi-Fi (AP) específico en una red inalámbrica.

```

$ sudo airodump-ng wlan0

CH 5 ][ Elapsed: 4 mins ][ 2023-05-12 10:49

BSSID            PWR  Beacons    #Data, #/s  CH  MB  ENC CIPHER  AUTH  ESSID
78:54:2E:B0:8B:E0 -1      0         29   0   3   -1  WPA
44:27:F3:B1:63:55 -84     4          0   0  11   65  WPA2 CCMP  PSK
00:26:B4:21:20:24 -84     3          0   0   1   54  WPA2 CCMP  PSK
62:E1:DC:A5:BC:BB -1      0          0   0  11   -1
52:32:F0:B2:FA:86 -82     7          0   0   6  180  WPA2 CCMP  PSK
A6:44:D1:FD:FA:F3 -85     2          0   0  13   65  WPA2 CCMP  PSK
FE:9F:C2:F7:A5:BD -70     2          0   0   1  195  WPA2 CCMP  PSK
46:D9:E7:23:A5:B2 -81    10          0   0   1  130  WPA2 CCMP  PSK
A4:2A:95:F6:16:95 -86     0          2   0   6  130  WPA2 CCMP  PSK
B8:D8:12:67:3B:68 -1      0          4   0   1   -1  WPA
56:D9:E7:23:A5:B2 -80    13          0   0   1  130  WPA2 CCMP  PSK
CC:2D:E0:3F:C5:ED -87     2          0   0   3  130  WPA2 CCMP  PSK
18:0F:76:EE:C6:D1 -82     0         31   0   1  130  WPA2 CCMP  PSK
18:0F:76:EE:C6:D0 -74     0          7   0   1   -1  OPN
F0:9F:C2:F7:A4:CD -1      0          0   0   6   -1
3C:CD:57:6F:DA:CE -88     8          0   0   1  130  WPA2 CCMP  PSK
A4:2A:95:F6:17:51 -80     0         55   0  11  130  WPA2 CCMP  PSK
18:0F:76:EE:C6:D5 -82     0         25   0   1  130  WPA2 CCMP  PSK

```

Figura 5-20 Ejemplo de enumeración activa de redes Wi-Fi (Promwad, s.f.)

5.4 Reconocimiento de las personas

Los empleados de una organización constituyen el vector de acceso más crítico para acceder a las redes de la organización, ya que suelen ser el eslabón más débil en la cadena de seguridad. El acceso a ellos suele ser por ataques de ingeniería social, siendo los vectores de ataque más comunes los siguientes (Rudra, 2025):

- **Phishing:** correo electrónico malicioso.
- **Spear-phishing:** phishing dirigido.
- **Vishing:** llamadas de voz.
- **Smishing:** ataques por SMS malicioso.

Al igual que en el resto de los ataques, la fase inicial de los ataques de ingeniería social es la recopilación de información o reconocimiento, que tratará de obtener información de la organización objetivo, así como de sus empleados (Rudra, 2025).

En esta fase se tratará de obtener la mayor cantidad de información posible (Arriols, 2018):

- Investigación de la organización: oficinas y localización física, sector de actividad, empresas colaboradoras, cadena de suministro, etc.
- Obtención del organigrama de la organización y la estructura en departamentos.
- Listado de empleados encuadrados en sus departamentos.
- Correos electrónicos de la organización. Públicos y expuestos en leaks.

Posteriormente se analiza la información recopilada para identificar (Arriols, 2018):

- Empleados clave o idóneos para ataques de spear-phishing.
- Empleados idóneos para ataques de vishing.
- Colaboradores y clientes útiles para suplantación.
- Próximos eventos de la empresa que puedan dar contexto a posibles campañas de phishing.

5.5 Superficie de exposición

A partir de un análisis riguroso de la información recopilada en todas las fases del reconocimiento es posible identificar la superficie de exposición de la organización. Esta superficie comprende el conjunto de activos visibles o potencialmente descubiertos desde el exterior, así como las vulnerabilidades y configuraciones erróneas que un adversario podría explotar para llevar a cabo un ataque; en otras palabras, es la superficie de ataque expuesta (Figura 5-21). Entre los elementos que suelen formar parte de esta superficie de exposición se encuentran (Trend Micro, 2025):

- Servidores y aplicaciones web conectadas a Internet.
- Sistemas y aplicaciones desatendidos.
- APIs inseguras u olvidadas.
- Software y librerías sin actualizar y con vulnerabilidades conocidas.
- Exposición de software de terceros con vulnerabilidades conocidas.
- Conocimiento de la cadena de suministro.
- Almacenamiento en la nube mal configurado (acceso abierto).
- Credenciales expuestas en Leaks o en el código.
- Publicación repositorios públicos de datos sensibles de la organización.
- Exposición de los empleados en redes sociales.

La monitorización regular de la superficie de exposición aporta beneficios a la seguridad de la organización, como (Trend Micro, 2025; Wenzler, 2022):

- Visibilidad completa de los activos visibles desde el exterior.
- Identificación de vulnerabilidades y fallos de configuración de estos activos.
- Priorización según el contexto del activo.
- Anticipación ante potenciales amenazas.

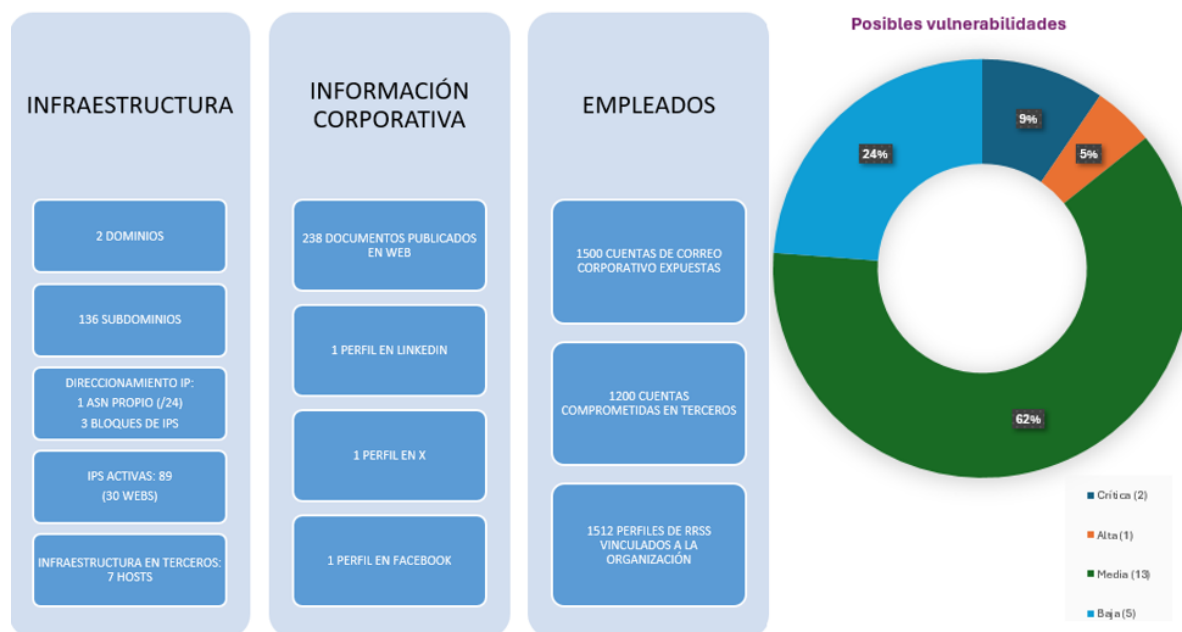


Figura 5-21 Ejemplo de superficie de exposición de una organización (elaboración propia)

El reconocimiento necesario para obtener la superficie de exposición es una tarea ardua y minuciosa. Para simplificar el proceso y automatizar la monitorización van apareciendo en el mercado diversas soluciones dedicadas, como la que se ve en la Figura 5-22 (CCN-CERT, 2024).

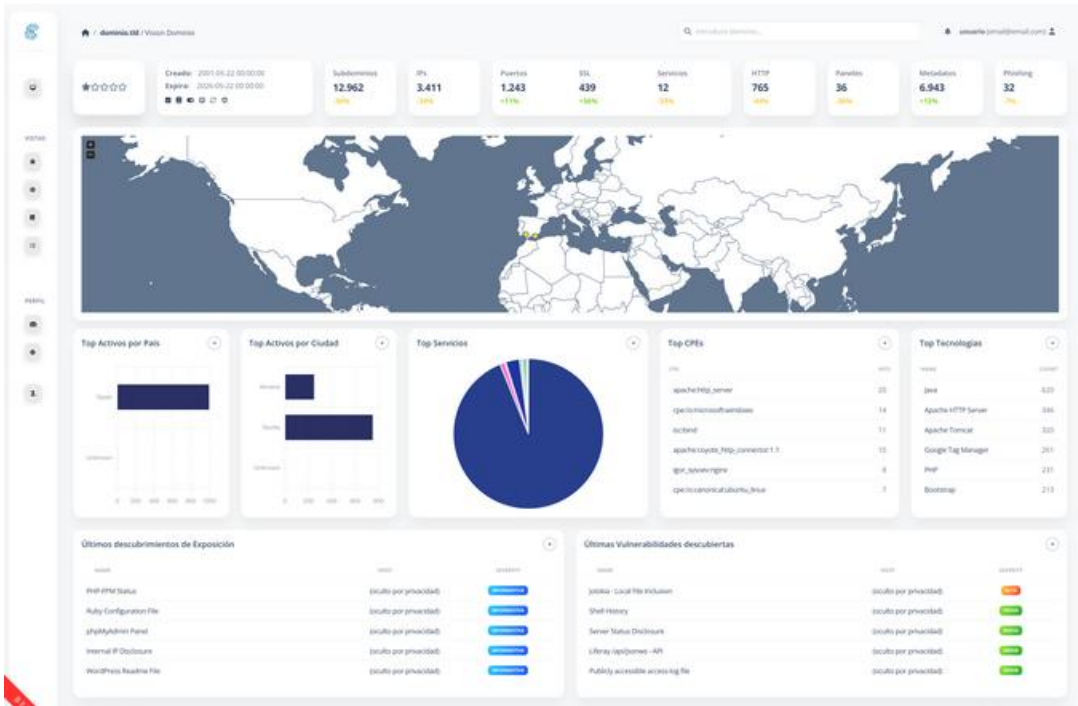


Figura 5-22 Vista del cuadro de mandos de la herramienta ELSA (CCN-CERT, s.f.)

5.6 Vectores de ataque

Una vez obtenida la superficie de exposición, el siguiente paso es identificar con esa información los vectores de ataque para entrar en ella (Figura 5-23). Se puede definir vector de ataque como la manera en la que un atacante puede tener acceso o conseguir los efectos deseados en la red o sistemas de una organización (Cutler, 2024).

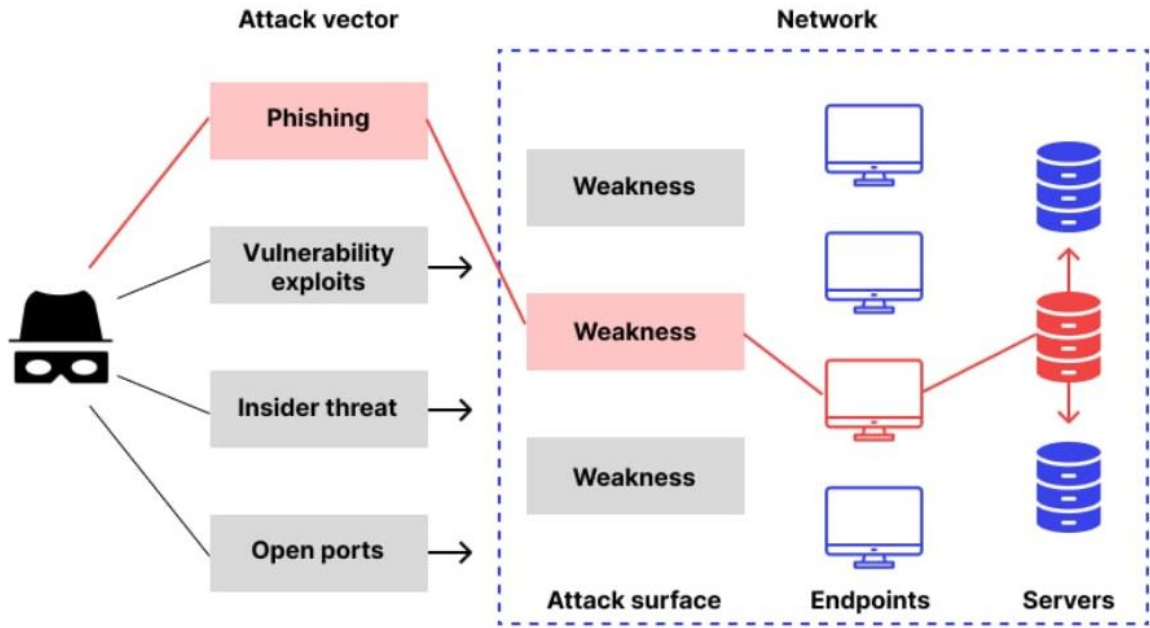


Figura 5-23 Selección de vectores de ataque (Lee, 2025)

Existen multitud de vectores de ataque, tantos como maneras en las que haya de entrar en una red, ya sea de manera física como virtual. La Tabla 5-6 muestra parte de ellos (LetsDefend, 2023).

Vector de ataque	Ejemplos	Objetivo	Identificador del Problema
Malware	Virus, gusano, troyano, spyware, rootkit	Robo de datos, robo de contraseñas, compromiso de red o sistema	Software antivirus; sistema de detección de intrusiones (IDS)
Phishing (incluye spear phishing)	Email malicioso engañoso con adjuntos o enlaces maliciosos	Acceso a red o sistema; brecha de datos	Usuario
Ransomware (incluye doxing)	Extorsión: datos eliminados o cifrados hasta pagar rescate	Extorsión para obtener rescate	Nota/anuncio de ransomware
DoS / DDoS	Saturar un dispositivo o servidor para impedir acceso	Interrupción de red o sistema	Administradores de red mediante monitoreo
Credenciales comprometidas/débiles/robadas	Cuenta y contraseña filtrada o robada	Brecha de datos	Investigación forense
Insider malicioso	Empleado descontento que expone información privada	Venganza, generar vergüenza	Dirección; US-CERT
Proveedores de terceros/cuarto nivel	Proveedores, socios de ciberseguridad	Obtener información competitiva	Monitoreo de red; gestión de logs
Cifrado inexistente o deficiente	Datos en reposo o tránsito	Acceder a datos	Evaluación del sistema
Mala configuración de dispositivos	Servidores, dispositivos de red, móviles	Acceso a dispositivo y datos	Evaluación del sistema
Vulnerabilidades sin parchear	Servidores, equipos de red, móviles	Acceder a dispositivo y datos	Gestión de parches
Inyecciones SQL	Manipulación de bases de datos para exponer info	Acceder a datos	Pentester
Cross-site scripting (XSS)	Inyección de código malicioso	Acceso a sistema, red y datos	Pentester

Secuestro de sesión	Intercepción de cookies de sesión	Acceder a datos	Usuario
Man-in-the-Middle (MitM)	Redes Wi-Fi públicas	Acceder a la red	IPS
Ataque de fuerza bruta	Intentos de prueba y error para obtener acceso	Acceso a red o sistema	Gestión de logs

Tabla 5-5 Ejemplos de vectores de ataque (LetsDefend, 2023)

Desde un punto de vista defensivo, el conocimiento de los vectores de acceso a la organización proporciona al Blue Team⁵⁰ el conocimiento de los puntos de entrada para poder simular los ataques de un potencial atacante, así como la priorización en el fortalecimiento de las defensas. Todo ello posibilita un enfoque de ciberseguridad proactiva (Alcarria, 2024). En la Tabla 5-7 se puede ver los vectores de ataque asociados a una vulnerabilidad encontrada.

ELEMENTO POTENCIALMENTE VULNERABLE	CATEGORÍA	CVEs ASOCIADOS	SEVERIDAD	VECTORES DE ATAQUE (Mitre ATT&K)	MITIGACIÓN (Mitre ATT&K)
Apache httpd sin actualizar (versión 2.4.41)	Servicios expuestos vulnerables	CVE-2020-13950	Crítica	T1190	M1051 Actualización del software
		CVE-2022-26377		Exploits contra Servidores y Aplicaciones web	
		CVE-2022-28330		TA0004 Escalada de Privilegios	M0937 - M1037 Filtrar tráfico de red
		CVE-2022-28614			
		CVE-2022-28615		T1499 Denegación de Servicio de Endpoint	M1038 Prevención de Ejecución de Código
		CVE-2022-29404			
		CVE-2022-30522			M1026 Gestión de privilegios
		CVE-2022-30556			
		CVE-2022-31813			M1048 Aislamiento de aplicaciones y Sandboxing
		CVE-2022-23943			
		CVE-2022-22721			
		CVE-2022-22720			
		CVE-2022-22719			
		CVE-2021-44790			
		CVE-2021-44224			
		CVE-2021-33193			
		CVE-2021-34798			
		CVE-2021-36160			
		CVE-2021-39275			
		CVE-2021-40438			
		CVE-2021-31618			
		CVE-2021-30641			
		CVE-2021-26691			
		CVE-2021-26690			
		CVE-2020-35452			
		CVE-2020-13950			
		CVE-2020-13938			
		CVE-2020-11984			
		CVE-2020-11993			
		CVE-2020-9490			
		CVE-2020-1934			
		CVE-2020-1927			
		CVE-2019-17567			

Tabla 5-6 Ejemplo de vulnerabilidad y vectores de ataque orientados a un Blue Team (elaboración propia)

⁵⁰ Blue Team: equipo defensivo que protege la red y responde a los ataques.

En la tabla anterior se pueden observar los vectores de ataque asociados a una vulnerabilidad desde un punto de vista defensivo. También se pueden diseñar los vectores de ataque en beneficio de un Red Team⁵¹ o equipo ofensivo (Cilleruelo, 2024b), como se puede observar en la Tabla 5-8.

TARGET: EMPRESA XYZ		
VECTOR DE ATAQUE	PUNTO DE ENTRADA	WEAPON/PAYLOAD
Spear Phishing	1.1 soyelceo@empresa.com	Email + Stealer ⁵²
	1.2 jefeoperaciones@empresa.com	Email + Stealer
	1.3 jeferrhh@empresa.com	Email + Stealer
Exploit ⁵³	2.1 IP:puerto – CVE 2025-012345 (Critical 9.9)	Exploit Superespia (CVE 2025-012345)
Ataque web	3.1 www.acceso.empresa.com/login	sqli
	3.2 www.campusvirtual.empresa.com/login	XSS reflected ⁵⁴
Ataque por credenciales	4.1 www.vpn.empresa.com/acceso	Password spraying ⁵⁵
	4.2 www.vpn.empresa.com/acceso	Fuerza bruta ⁵⁶

Tabla 5-7 Ejemplo de vectores de ataque orientados a un Red Team (elaboración propia)

5.7 Enumeración interna

En una operación CISRO intrusiva, una vez dentro de las redes del objetivo, el primer paso a realizar es recabar la mayor información posible de la red interna, como las máquinas activas, recursos compartidos, usuarios, dominios y grupos de trabajo. Esta fase es conocida como Enumeración (Astudillo, 2018; Fernández et al., 2011).

La información que se puede obtener dependerá de la red a la que se enfrente el atacante y a su estado de seguridad. Normalmente se suele analizar el directorio activo de Windows aprovechando técnicas de enumeración de protocolos como NetBIOS⁵⁷, DNS, LDAP⁵⁸, SNMP⁵⁹, SMTP⁶⁰ y HTTP (Astudillo, 2018).

⁵¹ Red Team: equipo ofensivo que simula ciberataques para identificar vulnerabilidades en los sistemas de una organización.

⁵² Tipo de malware diseñado para el robo de información.

⁵³ Código, software o técnica que se aprovecha de una vulnerabilidad de seguridad en un sistema, aplicación o dispositivo para causar un comportamiento inesperado, como obtener acceso no autorizado o ejecutar código malicioso.

⁵⁴ Tipo de ataque no persistente donde un atacante inyecta código malicioso (tipo JavaScript) a través de una URL o formulario.

⁵⁵ Técnica de ataque utilizada para comprometer cuentas aprovechando contraseñas débiles o comunes, pero sin disparar mecanismos de bloqueo por intentos fallidos.

⁵⁶ Intento de obtener acceso a una cuenta probando sistemáticamente todas las combinaciones posibles de credenciales.

⁵⁷ Protocolo que permite la comunicación entre equipos de una red de área local (LAN). Asocia nombres únicos a direcciones IP para que puedan encontrarse y compartir recursos.

⁵⁸ Protocolo ligero de acceso a directorios. Se utiliza para acceder y mantener servicios de directorio distribuidos a través de una red mediante autenticación centralizada.

⁵⁹ Protocolo Simple de Administración de Red (SNMP). Se utiliza para intercambiar información de administración entre dispositivos de red, como routers, switches y servidores.

⁶⁰ Protocolo Simple de Transferencia de Correo. Posibilita el envío de correos electrónicos a través de Internet.

La información que suele buscar el atacante dependerá de su objetivo, siendo algunos de los recursos más buscados los siguientes (Arriols, 2018; Fernández et al., 2011):

- Enumeración de máquinas.
 - Recursos compartidos de cada máquina.
 - Dominios accesibles de la red.
 - Máquinas encendidas pertenecientes a un dominio.
 - Recursos compartidos pertenecientes a un dominio.
- Identificación de subredes.
- Identificación de relaciones de confianza.
- Políticas de seguridad en las cuentas.
- Usuarios.
- Grupos del dominio y locales.
- Servicios activos en ejecución.
- Registro de Windows.

Si bien esta enumeración se puede hacer poco a poco ejecutando comandos del sistema operativo, existen herramientas que realizan esta enumeración de una manera automatizada como se puede ver en la Figura 5-24.

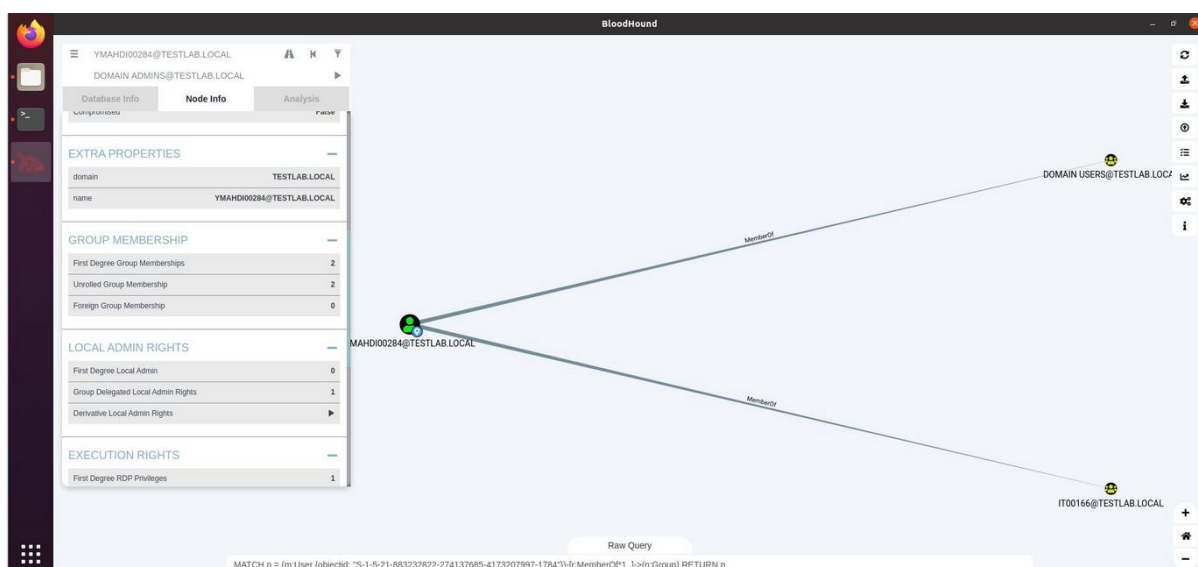


Figura 5-24 Ejemplo de enumeración automática con herramienta BloodHound (SANS Institute, 2021)

Toda esta información servirá para facilitar realizar los movimientos laterales de cara a seguir las siguientes fases de la Kill Chain. Las TTP de las operaciones CISRO intrusivas suelen ser clasificadas por lo que no es objeto de este estudio.

PÁGINA INTENCIONADAMENTE EN BLANCO

6 CONCLUSIONES Y LÍNEAS FUTURAS

6.1 Conclusiones

El presente Trabajo de Fin de Máster ha tenido como objetivo general revisar el estado del arte de las operaciones ISR en el ciberespacio y proponer una metodología que permita planificar y llevar a cabo este tipo de operaciones, identificando su marco doctrinal, así como sus procedimientos técnicos. A lo largo del desarrollo del trabajo se han abordado y conseguido los objetivos específicos planteados en la introducción.

En primer lugar, se ha descrito el marco doctrinal y organizativo que sustenta las operaciones en el ciberespacio, analizando el reconocimiento del ciberespacio como dominio de las operaciones militares por parte de la OTAN, la Unión Europea y España, así como los aspectos legislativos que afectan a las operaciones CISRO (OE1).

En segundo lugar, se han adaptado conceptos de la inteligencia clásica al ámbito ciberespacial, tomando como referencia la aproximación de la inteligencia de ciberamenazas (OE2).

Se han estudiado las técnicas de análisis estructurado que mejor se adecuan a la obtención de inteligencia sobre ciberataques, entre ellas MITRE ATT&CK, la Kill Chain y el Diamond Model. Se ha desarrollado además un caso práctico basado en la teoría de análisis de hipótesis competidoras (ACH), con el objeto de aportar una metodología aplicable al análisis y atribución de ciberataques (OE3).

Se han analizado las principales técnicas y metodologías de cibervigilancia, con especial mención a las diferentes disciplinas de obtención que emplea (OSINT, SOCMINT y VHUMINT), así como a los campos de actuación en el ciberespacio, como la Surface, Deep y Dark Web (OE4).

Por último, se ha examinado de manera conceptual las técnicas de reconocimiento pasivo y activo, proponiendo un procedimiento lógico y ordenado que permita obtener la superficie de exposición y la identificación de vectores de ataque (OE5).

Del análisis realizado se desprenden varios hallazgos significativos, los cuales se enumeran a continuación.

El ciclo de la inteligencia se puede aplicar al entorno ciberespacial orientándolo a la inteligencia de ciberamenazas. Esta inteligencia aporta valor al transformar los datos obtenidos en conocimiento accionable y útil para la toma de decisiones. El empleo de modelos como MITRE ATT&CK o el Diamond Model permite estructurar la información y correlacionar Tácticas, Técnicas y Procedimientos empleados por actores hostiles, posibilitando una comprensión más profunda y contextualizada de las amenazas, la identificación de campañas y, en algunos casos, la atribución de los incidentes. La inteligencia obtenida de los ataques en el ciberespacio tiene un ciclo de vida corto, por lo que debe compartirse de una manera rápida, estructurada y estandarizada para que pueda integrarse en las herramientas automatizadas de los SOC.

La cibervigilancia es un instrumento clave de alerta temprana, que permite identificar patrones de actividad hostil y amenazas incipientes. Su eficacia depende en gran medida de la integración de múltiples disciplinas de obtención y del seguimiento de actividades también en la Deep y Dark Web.

El reconocimiento se convierte en una capacidad indispensable para determinar la superficie de exposición digital de un objetivo y anticipar posibles vectores de ataque. Constituye la primera fase de la Cyber Kill Chain y se puede emplear tanto desde un enfoque defensivo, orientado a la propia organización, como ofensivo, dirigido contra un objetivo encomendado.

Todo ello pone de manifiesto que las tres capacidades estudiadas —inteligencia, cibervigilancia y reconocimiento— no deben entenderse como compartimentos estancos, sino como fases complementarias de un mismo proceso orientado a garantizar la superioridad de la información en el campo de batalla. Todo ello revierte en una defensa proactiva y en el conocimiento más profundo de los

adversarios en el campo de batalla digital. Por ello se puede concluir que las operaciones ISR en el ciberespacio (CISRO) constituyen un pilar esencial para identificar, anticipar y contrarrestar las amenazas en este dominio.

La aportación de este trabajo puede valorarse en dos planos. Desde una perspectiva académica, muestra una recopilación de conocimientos que hasta ahora aparecían de forma dispersa, integrando en un marco ISR las capacidades de inteligencia de ciberamenazas, cibervigilancia y reconocimiento. De esta manera se superan las aproximaciones fragmentarias y se ofrece una visión más completa del proceso ISR en su conjunto. Desde una perspectiva práctica, el estudio propone un marco de referencia útil para la planificación y conducción de operaciones ISR en el ciberespacio, reforzando las capacidades de anticipación, detección y mitigación de amenazas.

6.2 Líneas futuras

El trabajo presenta ciertas limitaciones. En primer lugar, se ha basado fundamentalmente en fuentes abiertas y doctrinales, lo que ha restringido el acceso a información clasificada, especialmente en lo relativo a las capacidades ofensivas. Por ello no se ha podido abordar en profundidad las operaciones CISRO intrusivas. En segundo lugar, el estudio se ha centrado principalmente en referencias de la OTAN, la Unión Europea y España, por lo que quedan fuera las aproximaciones de otros actores internacionales muy activos en operaciones de espionaje en el ciberespacio, como Rusia o China, cuya inclusión hubiese enriquecido el análisis. Estos hechos se podrían tener en cuenta para futuros estudios.

Además, se identifican otras líneas de investigación futura que permitirían profundizar en el estudio de las operaciones ISR en el ciberespacio y en las que será más fácil encontrar información.

Una primera línea se orientaría al análisis de la aportación de las CISRO a las operaciones conjuntas y combinadas multidominio, con el fin de mostrar las ventajas de la combinación de acciones en el ciberespacio para conseguir efectos cinéticos.

Otra vía de investigación consistiría en estudiar la contribución de las CISRO al ciclo de targeting, en particular en lo relativo al desarrollo de targets virtuales, la estimación de efectos colaterales (Collateral Damage Estimation, CDE) y la valoración de daños tras un ataque (Battle Damage Assessment, BDA), campo en el que no existe apenas doctrina adaptada al ciberespacio.

Por último, resulta de gran interés profundizar en la integración de tecnologías emergentes como la inteligencia artificial, el machine learning o el big data, que sin duda aportarán un gran valor a la mejora de la monitorización, correlación de amenazas y la toma de decisiones.

7 BIBLIOGRAFÍA

- Abrams, L. (2020). *Hacker leaks 386 million user records from 18 companies for free*. Recuperado de <https://www.bleepingcomputer.com/news/security/hacker-leaks-386-million-user-records-from-18-companies-for-free/>
- Acqnotes. (s.f.). *Information Technology. Cyberspace*. Recuperado de <https://acqnotes.com/acqnote/careerfields/cyberspace>
- Akamai. (2024). *Análisis de dominios maliciosos que suplantan la identidad de CrowdStrike: afectados y previsiones de futuro*. Recuperado de <https://www.akamai.com/es/blog/security-research/2024-july-crowdstrike-bsod-domains-what-could-come-next>
- Alcarria, P. (2024). *Ciberseguridad proactiva: La importancia del Blue Team*. Recuperado de <https://openwebinars.net/blog/ciberseguridad-proactiva-la-importancia-del-blue-team/>
- Altvater, L. (s.f.). *Traffic Light Protocol (TLP)*. RCTS CERT. Recuperado de https://www.cert.rcts.pt/images/CiaB2022/Actividade_07_Traffic_Light_Protocol.pdf
- Álvarez, E. (2022). *La ICANN lanza una nueva herramienta para verificar la conformidad con los requisitos del RDAP*. Internet Corporation for Assigned Names and Numbers. Recuperado de <https://www.icann.org/es/blogs/details/icann-launches-new-tool-to-verify-conformance-with-rdap-requirements-3-2-2022-es>
- Álvarez, I. (2019). *El derecho del ciberespacio. Una aproximación*. Recuperado de <https://vlex.es/vid/derecho-ciberespacio-aproximacion-839283171>
- Amin, R., Cloppert, M. & Hutchins, E. (s.f.). *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*. Recuperado de <https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf>
- Ardal, A. (2025). *Three Pillars of Threat Intelligence: Kill Chain, MITRE ATT&CK, and the Diamond Model*. Recuperado de <https://medium.com/@aliardal/three-pillars-of-threat-intelligence-kill-chain-mitre-att-ck-and-the-diamond-model-7505315bbec5>
- Arriols, E. (2018). *Chief Information Security Officer. El Red Team de la empresa*. Móstoles, España: 0xWORD.
- Arrollo, B., & Volpe, M. (2025). *Telegram Intelligence: Guía inicial para analistas*. Recuperado de <https://ciberprisma.org/2025/04/20/telegram-intelligence-guia-inicial-para-analistas/>
- Astudillo, K. (2018). *Hacking ético. 3ª edición*. Madrid, España: Ra-Ma.
- Badger, L., Johnson, C., Skorupka, C., Snyder, J. & Waltermire, D. (2016). *NIST Special Publication 800-150. Guide to Cyber Threat Information Sharing*. National Institute of Standards & Technology. Recuperado de <http://dx.doi.org/10.6028/NIST.SP.800-150>
- Bahrami, P., Benedetto, L., Bianchi, G., Conti, M., Dargahi, T. & Dehghantanha, A. (2019). *A Cyber-Kill-Chain based taxonomy of crypto-ransomware features*. Recurepado de <https://doi.org/10.1007/s11416-019-00338-7>
- Baker, K. (2025a). *Cyber Threat Intelligence Explained*. Recuperado de <https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/>

- Baker, K. (2025b). *Indicators of Compromise (IOC) Security Explained*. Recuperado de <https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/indicators-of-compromise-ioc/>
- Bazzell, M. (2019). *Open Source Intelligence Techniques. Resources for searching and analyzing online information. Seventh edition*. Gran Bretaña: Amazon.
- Bederov, I. (2022). *OSINT in VKontakte*. Recuperado de <https://medium.com/@ibederov/en/osint-in-vkontakte-739e0276f545>
- Benedetti, W. (2011). *Hacking group LulzSec says it takes out CIA website*. Recuperado de <https://www.nbcnews.com/tech/tech-news/hacking-group-lulzsec-says-it-takes-out-cia-website-flna122798>
- Bernabe, J., Joosen, W., Preuveneers, D & Skarmeta, A. (2020). *Distributed Security Framework for Reliable Threat Intelligence Sharing*. Recuperado de <http://dx.doi.org/10.1155/2020/8833765>
- Bertriu, C. (2013). *El amor y el odio del FBI con Anonymous*. Recuperado de <https://www.elmundo.es/elmundo/2013/08/26/navegante/1377494915.html>
- Bianco, D. (2025). *The Pyramid of Pain*. Recuperado de <https://www.sans.org/tools/the-pyramid-of-pain>
- Blanco, J.L. (2021). *Operaciones defensivas en el Ciberespacio*. Recuperado de <https://www.elradar.es/operaciones-defensivas-en-el-ciberespacio/>
- Bugcrowd. (s.f.). *Nessus® Vulnerability Scanner*. Recuperado de <https://www.bugcrowd.com/glossary/nessus-vulnerability-scanner/>
- Bytemind. (2021). *DNS enumeration – técnicas y herramientas*. Recuperado de <https://byte-mind.net/dns-enumeration-tecnicas-y-herramientas/>
- Caltagirone, S., Pendergast, A. & Betz, C. (2013). *The Diamond Model of Intrusion Analysis*. Recuperado de <http://dx.doi.org/10.13140/RG.2.2.31143.56481>
- Carles, J. (2016). *¿Qué es y cómo funciona la red Tor para mejorar nuestra privacidad?* Recuperado de <https://geekland.eu/que-es-y-como-funciona-la-red-tor/>
- CCAS. (2020). *Investigation of Facebook related crimes*. Recuperado de <https://blog.ccasociety.com/investigation-of-facebook-related-crimes/>
- CCDCOE. (2020). *Cyber Commanders' Handbook*. Tallin. NATO Cooperative Cyber Defence Centre of Excellence.
- CCN. (2012). *Guía de seguridad (CCN-STIC-822). Procedimiento de seguridad en el ENS. Anexo II. Procedimiento de clasificación y tratamiento de la información clasificada. PR20*. Madrid. Centro Criptológico Nacional. Recuperado de <https://www.ccn-cert.cni.es/gl/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/539-ccn-stic-822-procedimientos-de-seguridad-anexo-ii/file.html>
- CCN. (2015). *Guía de seguridad (CCN-STIC-425). Ciclo de inteligencia y análisis de intrusiones*. Madrid. Centro Criptológico Nacional.
- CCN. (2021). *Guía de Seguridad de las TIC CCN-STIC 201. Organización y Gestión para la Seguridad de las TIC*. Madrid. Centro Criptológico Nacional. Recuperado de <https://www.ccn-cert.cni.es/es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/45-ccn-stic-201-estructura-de-seguridad/file?format=html>
- CCN-CERT. (2024). *El CCN-CERT inicia un proyecto piloto para medir la superficie de exposición de la Administración Pública a través de ELSA, su nueva herramienta*. Centro Criptológico Nacional. Recuperado de <https://www.ccn-cert.cni.es/es/seguridad-al-dia/novedades-ccn->

[cert/12890-el-ccn-cert-inicia-un-proyecto-piloto-para-medir-la-superficie-de-exposicion-de-la-administracion-publica-a-traves-de-elsa-su-nueva-herramienta.html](https://www.ccn-cert.cni.es/es/soluciones-seguridad/elsa.html)

CCN-CERT. (s.f.). *ELSA*. Centro Criptológico Nacional. Recuperado de <https://www.ccn-cert.cni.es/es/soluciones-seguridad/elsa.html>

Ciberseguridad. (s.f.). *Guía definitiva de I2P: cómo instalarlo y usarlo*. Recuperado de <https://ciberseguridad.com/guias/recursos/i2p/#%C2%BFComo funciona>

Cibervoluntarios. (2022). *¿Qué es Telegram y para qué puedes usarlo?* Recuperado de <https://www.publico.es/sociedad/telegram-puedes-usarlo.html>

Cilleruelo, C. (2024a). *¿Qué es fuzzing?* Recuperado de <https://keepcoding.io/blog/que-es-fuzzing-ciberseguridad/>

Cilleruelo, C. (2024b). *Vectores de acceso en un ejercicio Red Team*. Recuperado de <https://keepcoding.io/blog/vectores-de-acceso-en-un-ejercicio-red-team/>

Codera, G. (2021). *Los espías que usan LinkedIn para robar secretos de empleados gubernamentales*. Recuperado de <https://www.bbc.com/mundo/noticias-56836719>

Comodo. (s.f.). *WHAT IS SOC (Security Operation Center)?* Recuperado de <https://www.comodo.com/soc-network.php>

CQCore, evandrodacs & Rogov, M. (2025). *Telegram-OSINT*. Recuperado de <https://github.com/The-OSint-Toolbox/Telegram-OSINT>

Cutler, A., Trevino, A. & Guccione, D. (2024). *Ocho vectores de ataque habituales que las organizaciones deben conocer*. Recuperado de <https://www.keepersecurity.com/blog/es/2024/04/04/eight-common-attack-vectors-organizations-need-to-be-aware-of/>

Cyber Mentor. (s.f.). *OSINT: Qué es, Aspectos Éticos y Áreas de Aplicación*. Recuperado de <https://cybermentor.net/osint-que-es-aplicacion/>

Darknetsearch. (2025). *Ciberseguridad en 2025: La importancia de la monitorización de la dark web y la detección de filtraciones*. Recuperado de <https://darknetsearch.com/knowledge/news/es/monitorizacion-de-la-dark-web>

Darley, T., Jordan, B. & Piazza, R. (2021). *STIX Version 2.1*. Recuperado de <https://www.oasis-open.org/standard/6426/>

Davidson, M., Jordan, B. & Wunder, J. (2017). *TAXII™ Version 2.0. Committee Specification 01*. Recuperado de <https://docs.oasis-open.org/cti/taxii/v2.0/cs01/taxii-v2.0-cs01.html>

Dean. (2024). *Cyber Attribution*. Recuperado de <https://enclaveconsulting.co.uk/cyber-attribution/>

DeBolt, M. (2023). *Gaining the Intelligence Advantage with Cyber HUMINT - Part One*. Recuperado de <https://intel471.com/blog/gaining-the-intelligence-advantage-with-cyber-humint-part-one>

DSN. (2019). *Estrategia Nacional de Ciberseguridad 2019*. Madrid. Ministerio de la Presidencia, Relaciones con las Cortes e Igualdad. Recuperado de <https://www.dsn.gob.es>

Dulaunoy, A., Iklody, A., Wagener, G. & Wagner, C. (2016). *MISP - The Design and Implementation of a Collaborative Threat Intelligence Sharing Platform*. Recuperado de <https://dl.acm.org/doi/10.1145/2994539.2994542>

EMAD. (2011a). *Visión del JEMAD de la Ciberdefensa Militar*. Madrid. Estado Mayor de la Defensa.

EMAD. (2011b). *Concepto de Ciberdefensa Militar*. Madrid. Estado Mayor de la Defensa.

- EMAD. (2012). *Plan de Acción para la Obtención de la capacidad de Ciberdefensa Militar*. Madrid. Estado Mayor de la Defensa.
- EMAD. (2018). *Concepto de Ciberdefensa. Resumen ejecutivo*. Madrid. Estado Mayor de la Defensa.
- EMAD. (2020). *PDC-2. Doctrina de Inteligencia para las FAS*. Madrid. Estado Mayor de la Defensa.
- ENISA. (2024). *ENISA Threat Landscape 2024. European Union Agency for Cybersecurity*. Recuperado de <https://www.enisa.europa.eu/topics/cyber-threats/threat-landscape>
- Enthec. (2024). *¿Qué es un CVE?* Recuperado de <https://enthec.com/que-es-un-cve/>
- ESFAS. (2014). *Estrategia de la información y seguridad en el ciberespacio. Documentos de Seguridad y Defensa 60*. Madrid. Ministerio de Defensa.
- Esgeeks. (s.f.). *Geogramint: Una Herramienta OSINT de Geolocalización para Telegram*. Recuperado de <https://esgeeks.com/geogramint-osint-geolocalizacion-telegram/>
- EUROPOL. (2025). *Global operation targets NoName057(16) pro-Russian cybercrime network*. Agencia de la Unión Europea para la Cooperación Policial. Recuperado de <https://www.europol.europa.eu/media-press/newsroom/news/global-operation-targets-noname05716-pro-russian-cybercrime-network>
- EUROPOL. (s.f.). *Cybercrime*. European Union Agency for Law Enforcement Cooperation. Recuperado de <https://www.europol.europa.eu/crime-areas/cybercrime>
- Fernández, Y. (2021). *Red TOR: qué es, cómo funciona y cómo se usa*. Recuperado de <https://www.xataka.com/basics/red-tor-que-como-functiona-como-se-usa>
- Fernández, Y. (2024). *Deep Web, Dark Web y Darknet: éstas son las diferencias*. Recuperado de <https://www.xataka.com/servicios/deep-web-dark-web-darknet-diferencias>
- Fernández, Y., García-Moran, J.P., Martínez, R., Ochoa, A., & Ramos, A.A. (2011). *Hacking y Seguridad en Internet. Edición 2011*. Paracuellos de Jarama, España: Ra-Ma.
- Filigran. (s.f.). *OpenCTI. Understand Your Threat Landscape and Act Decisively*. Recuperado de <https://filigran.io/platforms/opencti/>
- FIRST. (s.f.a). *Common Vulnerability Scoring System version 4.0: Specification Document. Document Version: 1.2*. Forum of Incident Response and Security Teams. Recuperado de <https://www.first.org/cvss/v4-0/specification-document>
- FIRST. (s.f.b). *TLP:CLEAR. Protocolo de Luces de Semáforo - Traffic Light Protocol (TLP). Versión 2.0. Definiciones y guías de uso de los estándares FIRST*. Forum of Incident Response and Security Teams. Recuperado de <https://www.first.org/tlp/docs/v2/TLP-ESv4.pdf>
- Fortinet. (2025). *¿Qué es el ciberespionaje?*. Recuperado de <https://www.fortinet.com/lat/resources/cyberglossary/cyber-espionage>
- Frayssinet, M. (2024). *Cyber Threat Intelligence (CTI) - Parte 2 OpenCTI*. Recuperado de <https://es.linkedin.com/pulse/cyber-threat-intelligence-cti-parte-2-opencti-frayssinet-delgado-y8gee>
- Fuente, I. (2022). *Ciberespacio: un nuevo dominio para las operaciones*. Recuperado de https://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Nacional/LaOTAN_ciberespacio.pdf
- Fyodor, G. (2008). *NMAP Network Scanning: Official Nmap Project Guide to Network Discovery and Security Scanning*. Sunnyvale, Estados Unidos: Insecure.com LLC.
- GeeksforGeeks. (2024). *Computer Emergency Response Team (CERT)*. Recuperado de <https://www.geeksforgeeks.org/computer-emergency-response-team-cert/>

- Geeksforgeeks. (2025). *What is UDP Scanning?* Recuperado de <https://www.geeksforgeeks.org/ethical-hacking/what-is-udp-scanning/>
- Genez, G. (2020). *Freenet: conoce cómo funciona esta red alternativa a Tor*. Recuperado de <https://seguridadpy.info/2020/11/freenet-conoce-como-functiona-esta-red-alternativa-a-tor/>
- Guerra, M. (2023). *Ciberinteligencia de la amenaza en entornos corporativos*. Paracuellos de Jarama, España: Ra-Ma.
- Ghimiray, D. (2024). *¿Qué es el navegador Tor?* Recuperado de <https://www.avast.com/es-es/c-tor-dark-web-browser>
- Goberna. (2025). *¿Qué es SOCMINT? Inteligencia en redes sociales en tiempo real*. Recuperado de <https://grupogoberna.com/que-es-socmint-inteligencia-en-redes-sociales/>
- Goedegebure, C. (2018). *TCP 3-way handshake and port scanning*. Recuperado de <https://www.coengoedegebure.com/tcp-3-way-handshake-port-scanning/>
- Goss, A. (2024). *Collection Management Framework: How to Manage Your Data Sources*. Recuperado de <https://kravensecurity.com/collection-management-framework/>
- Goss, A. (2025). *Nmap Ping Sweep: How to Scan Networks for Live Hosts*. Recuperado de <https://www.stationx.net/nmap-ping-sweep/>
- Goździewicz, W. (2019). *Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA)*. Recuperado de <https://www.cyberdefensemagazine.com/sovereign-cyber/>
- Greenberg, A. (2019). *Sandworm: a new era of cyberwar and the Hunt for the Kremlin's most dangerous hackers*. Nueva York, Estados Unidos: Doubleday.
- Huarui, Z. (2022). *DataWorks Data Analysis Module*. Recuperado de https://www.alibabacloud.com/blog/dataworks-data-analysis-module_598666
- Hyden, J. (2025). *Diferentes grados de clasificación en los documentos*. Recuperado de <https://www.lisanews.org/inteligencia/diferentes-grados-de-clasificacion-en-los-documentos/>
- IEEE. (2020). *Documento de Trabajo 01/2020. Implicaciones del ámbito cognitivo en las Operaciones Militares*. Madrid. Instituto Español de Estudios Estratégicos. Centro Superior de Estudios de la Defensa Nacional. Recuperado de https://emad.defensa.gob.es/Galerias/CCDC/files/IMPLICACIONES_DEL_AMBITO_COGNITIVO_EN_LAS_OPERACIONES_MILITARES.pdf
- Ikusi. (s.f.). *¿Qué es Threat Hunting y por qué es necesario tenerlo?* Recuperado de <https://www.ikusi.com/mx/blog/threat-hunting/>
- INCIBE. (2024). *La guardia Civil detiene a tres hacktivistas prorrusos del grupo NoName057(16)*. Instituto Nacional de Ciberseguridad. Recuperado de <https://www.incibe.es/incibe-cert/publicaciones/bitacora-de-seguridad/la-guardia-civil-detiene-tres-hacktivistas-prorrusos-del-grupo>
- INCIBE. (s.f.). *Vulnerabilidades*. Instituto Nacional de Ciberseguridad. Recuperado de <https://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades>
- Infobae. (2019). *China usa LinkedIn para reclutar espías en el extranjero*. Recuperado de <https://www.infobae.com/america/mundo/2019/08/28/china-usa-linkedin-para-reclutar-espias-en-el-extranjero/>
- IritT. (2024). *TheHive Project — SOC Level 1 -Digital Forensics and Incident Response — TryHackMe Walkthrough & Insights*. Recuperado de <https://iritt.medium.com/thehive-project-soc-level-1-digital-forensics-and-incident-response-tryhackme-walkthrough-713c89aa5c6f>

- IT Digital Security. (2023). *Falsos dominios: cómo se crean, cómo se distribuyen y para qué*. Recuperado de <https://www.itdigitalsecurity.es/actualidad/2023/06/falsos-dominios-como-se-crean-como-se-distribuyen-y-para-que>
- IUCPOL. (2023). *¿Qué es la HUMINT?* Recuperado de https://iucpol.com/que-es-la-humint/?srsltid=AfmBOop5_FkIXXXtSEvIxlQpPafn7-R3J3SJEHjDB-Aj8PAJEfhsgs
- Jain, S. (2024). *Cyber Alliance Threatens Major U.S. Energy Firms: High Society and Cyber Army of Russia Collaborate*. Recuperado de <https://thecyberexpress.com/cyber-army-of-russia-affiliate-high-society/>
- Jiménez, J. (2023). *I2P vs Tor: conoce las principales diferencias*. Recuperado de <https://www.redeszone.net/tutoriales/internet/i2p-tor-ventajas-anonimato/>
- Jiménez, J. (2025). *Evita que te ataquen los bots en redes sociales*. Recuperado de <https://www.redeszone.net/tutoriales/seguridad/detectar-bots-redes-sociales/>
- Kaminsky, S. (2023). *Dominios similares y cómo detectarlos*. Recuperado de <https://www.kaspersky.es/blog/lookalike-domains-in-bec/29038/?srsltid=AfmBOopjlcJLI5S-5IT8APOxoEphgFmjVf-tJrwWRHnRwcmTn301-MO>
- Kaspersky. (s.f.). *¿Qué es el cibercrimen? Cómo protegerse del cibercrimen*. Recuperado de <https://latam.kaspersky.com/resource-center/threats/what-is-cybercrime?srsltid=AfmBOor9o6spm-8-Ne2Iyw2ElIZFFWxMpvL6RjXZ7IIgEcUdJ4eV8pCy>
- Kurose, J.F & Ross, K.W. (2010). *Redes de computadoras. Un enfoque descendente*. 5ª Edición. Madrid, España: Pearson.
- Laprovittera, C. (2024). *OSINT #5 INSTAGRAM*. Recuperado de <https://achirou.com/osint-5-instagram/>
- Lee, I. (2025). *Attack vector - What is it? Definition & Examples*. Recuperado de <https://www.wallarm.com/what/attack-vector>
- Lee, Robert. M., Miller, B. & Stacey, M. *Collection Management Frameworks – Looking Beyond Asset Inventories in Preparation for and Response to Cyber Threats*. Recuperado de https://www.dragos.com/wp-content/uploads/CMF_For_ICS.pdf
- LetsDefend. (2023). *Cyber Security Attack Vectors*. Recuperado de https://py.linkedin.com/posts/letsdefend_cyber-security-attack-vectors-activity-7017140981275734016-REvX
- Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia. (2002). *Boletín Oficial del Estado*, (108), 16289–16293.
- Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. (1995). *Boletín Oficial del Estado*, (281), 33987–34058.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. (2018). *Boletín Oficial del Estado*, (294), 119788–119857.
- Ley Orgánica 5/2005, de 17 de noviembre, de la Defensa Nacional. (2005). *Boletín Oficial del Estado*, (276), 38770–38775.
- Lincoln, J. (2015). *Why You Should Be Using FollowerWonk for SEO and Social Media Success*. Recuperado de <https://ignitevisibility.com/followerwonk/>
- Lisa Institute. (2023). *SOCMINT o Inteligencia de Redes Sociales: qué es y para qué sirve*. Recuperado de <https://www.lisanews.org/inteligencia/socmint-o-inteligencia-de-redes-sociales-que-es-y-para-que-sirve/>

- Lisa Institute. (s.f.a). *Hactivismo: definición, tipos, modus operandi y motivaciones*. Recuperado de https://www.lisainstitute.com/blogs/blog/hactivismo-definicion-tipos-modus-operandi-motivaciones?srsId=AfmBOornG_gUHpkjnmuwSy59lfyCP_nDZN81RwssokCHJcfdqLFohDw8
- Lisa Institute. (s.f.b). *OSINT (Inteligencia de Fuentes Abiertas): tipos, métodos y salidas profesionales*. Recuperado de <https://www.lisainstitute.com/blogs/blog/osint-inteligencia-fuentes-abiertas?srsId=AfmBOorvt6rSi8aBbNGOGnNTToX9kwGtZDJ52q3r7bK2BuLrs-mS4GFru>
- Loading. (2024). *Qué es la base de datos Whois y para qué sirve*. Recuperado de <https://www.loading.es/blog/que-es-la-base-de-datos-whois-y-para-que-sirve/>
- Lockheed Martin. (s.f.). *The Cyber Kill Chain*. Recuperado de <https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>
- López, A. (2015). *Métricas de evaluación de vulnerabilidades: CVSS 3.0*. Instituto Nacional de Ciberseguridad. Recuperado de <https://www.incibe.es/incibe-cert/blog/cvss3-0>
- Loyalonlytoday. (2025). *Telegram bots for OSINT*. Recuperado de <https://osintteam.blog/telegram-bots-for-osint-fd74575e8ff3>
- Malwarebytes. (s.f.). *¿Qué es la vigilancia de la web oscura y cómo funciona?* Recuperado de <https://www.malwarebytes.com/es/cybersecurity/basics/dark-web-monitoring>
- Martin, A. (2022). *Cibervigilancia contra las nuevas amenazas*. Recuperado de <https://ifgeekthen.nttdata.com/s/post/cibervigilancia-contra-las-nuevas-amenazas-MCNMIDCMU5NVHPDB2JQMZYK37J7Q?language=es>
- Martín, S. (2025a). *Las redes sociales más utilizadas en el mundo y en España [2025]*. Recuperado de <https://mkparadise.com/redes-sociales-mas-utilizadas>
- Martín, S. (2025b). *Qué es LinkedIn, para qué sirve y cómo funciona*. Recuperado de <https://metricool.com/es/que-es-linkedin/>
- Martínez, A. (2014). *OSINT - La información es poder*. Instituto Nacional de Ciberseguridad. Recuperado de <https://www.incibe.es/incibe-cert/blog/osint-la-informacion-es-poder>
- Martínez, A. (2022). *Los ataques más impactantes de Anonymous en su historia*. Recuperado de <https://www.gq.com.mx/entretenimiento/articulo/anonymous-y-sus-ataques-mas-importantes>
- MB Secure. (2019). *DeTT&CT: Mapping your Blue Team to MITRE ATT&CK*. Recuperado de <https://www.mbsecure.nl/blog/2019/5/dettact-mapping-your-blue-team-to-mitre-attack>
- McCandless, D., Evans, T., & Barton, P. (2024). *World's Biggest Data Breaches & Hacks*. Recuperado de <https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>
- McNab, C. (2017). *Network Security Assessment. Know your network. 3° Edition*. Sebastopol, Estados Unidos: O'Reilly.
- Méndez, B. (2022). *Cumbre de la OTAN: la Policía monitoriza redes por temor a los antisistema y prorrusos*. Recuperado de <https://www.vozpopuli.com/actualidad/cumbre-otan-policia-amenazas.html>
- Ministerio de Defensa de España. (2023). *Orden DEF/1110/2023, de 4 de octubre, por la que se modifica la Orden DEF/710/2020, de 27 de julio, por la que se desarrolla la organización básica del Estado Mayor de la Defensa*. Boletín Oficial del Estado. Recuperado de https://noticias.juridicas.com/base_datos/Admin/774181-om-def-1110-2023-de-4-oct-modifica-la-om-def-710-2020-de-27-jul-por-la-que.html

- Moore, D. (2021). *Offensive Cyber Operations. Understanding Intangible Warfare*. Nueva York, Estados Unidos: Oxford University Press.
- NATO. (2020). *NATO Standard AJP-3.20. Allied Joint Doctrine for Cyberspace Operations. Edition A, Version 1*. North Atlantic Treaty Organization. Recuperado de https://assets.publishing.service.gov.uk/media/5f086ec4d3bf7f2bef137675/doctrine_nato_cyberspace_operations_ajp_3_20_1.pdf
- NATO. (2024a). *Cyber defence*. North Atlantic Treaty Organization. Recuperado de https://www.nato.int/cps/en/natohq/topics_78170.htm
- NATO. (2024b). *Countering hybrid threats*. North Atlantic Treaty Organization. Recuperado de https://www.nato.int/cps/en/natohq/topics_156338.htm.
- NIST. (s.f.). *National Vulnerability Database*. National Institute of Standards & Technology. Recuperado de <https://nvd.nist.gov/vuln>
- OKDiario (2015). Cómo saber si una cuenta de Twitter es falsa. Recuperado de <https://okdiario.com/tecnologia/como-saber-si-cuenta-twitter-falsa-2606411>
- OSINT Industries. (2025). *OSINT on VK: Find Russian Emails, Phone Numbers and More*. Recuperado de <https://www.osint.industries/post/osint-on-vk-find-russian-emails-phone-numbers-and-more>
- Pérez, P & Rego, M. (2016). *Cuadernos de Estrategia 185. Ciberseguridad: La cooperación público-privada. Capítulo cuatro. El intercambio de información de ciberamenazas*. Ministerio de Defensa. Recuperado de https://www.ieee.es/Galerias/fichero/cuadernos/CE_185.pdf
- Pinkowska, M. (2024). ¿Qué es la monitorización de la reputación de marca? Herramientas, consejos y mucho más [2025]. Recuperado de <https://brand24.com/blog/es/herramientas-de-monitorizacion-de-la-reputacion-de-marca/>
- Piña, R. (2025). *España, víctima favorita de los 'hacktivistas' prorrusos y de su batallón de élite, NoName057(16), por su apoyo a Ucrania*. Recuperado de <https://www.elmundo.es/espana/2025/01/03/67783634e4d4d8fc268b458a.html>
- Pointing, K. (s.f.). *REST Assured: Penetration Testing REST APIs Using Burp Suite: Part 2 – Testing*. Recuperado de <https://www.mindpointgroup.com/blog/rest-assured-penetration-testing-rest-apis-using-burp-suite-part-2-testing>
- Portillo, I. (2019). *Descubriendo que son los Data Leaks y los Data Breaches*. Recuperado de <https://derechodelared.com/2019/10/17/data-leaks-data-breaches/>
- Promwad. (s.f.). *Security Check for a Wi-Fi Access Point*. Recuperado de <https://promwad.com/case-studies/access-point-vulnerability-scanning>
- Radware. (s.f.). *LulzSec*. Recuperado de <https://www.radware.com/security/ddos-knowledge-center/ddospedia/lulzsec/>
- Rawrdcore. (s.f.). *TOOLS FOR OSINT VKONTAKTE*. Recuperado de <https://github.com/rawrdcore/vk-osint-en>
- Recorded Future. (2022). *The Intelligence Handbook. A Roadmap for Building an Intelligence-Led Security Program. Fourth Edition*. Annapolis, Estados Unidos: Cyber-Edge.
- Regalado, N. (s.f.). *¿Qué es Facebook, para qué sirve y cómo funciona esta red social?* Recuperado de <https://webescuela.com/facebook-que-es-como-funciona/>
- Rigall, M. (2024). *TFG: Sistema de detección de bots en redes sociales*. Recuperado de <https://iveres.es/tfg-sistema-de-deteccion-de-bots-en-redes-sociales/>

- Rodríguez, E. (2017). *Qué son las redes I2P: el Internet invisible*. Recuperado de https://www.elespanol.com/omicrono/20170727/redes-i2p-internet-invisible/234477787_0.html
- Romford, J. (2025). *Understanding PMESII-PT Analysis - Templates, Examples & More*. Recuperado de <https://agilityportal.io/blog/pmesii-pt-analysis>
- Rudra, A. (2025). *Ingeniería Social: Reconocer y prevenir ataques*. Recuperado de <https://powerdmarc.com/es/what-is-social-engineering/>
- Ruiz, A. (2024). *Efectivos del Mando del Ciberespacio blindarán también las elecciones europeas*. El Confidencial Digital. Recuperado de <https://www.elconfidencialdigital.com/articulo/defensa/militares-mando-ciberespacio-tambien-blindaran-elecciones-europeas/20240608000000794584.html>
- Ruiz, J. (2024). *Comunicación estratégica en las fuerzas armadas españolas*. Centro Superior de Estudios de la Defensa Nacional. Recuperado de <https://www.defensa.gob.es/ceseden/-/comunicaci%C3%B3n-estrat%C3%A9gica-en-las-fuerzas-armadas-esp%C3%B1olas-1>
- S2Grupo. (2024). *Hacktivismo: qué es y cuáles son sus motivaciones*. Recuperado de <https://s2grupo.es/hacktivismo-que-es-y-cuales-son-sus-motivaciones/>
- S2Grupo. (s.f.). *Cibervigilancia*. Recuperado de <https://s2grupo.es/soluciones/cibervigilancia/>
- San José, J. (2022a). *OpenCTI, Plataforma abierta de inteligencia sobre ciberamenazas*. Recuperado de <https://derechodelared.com/2022/10/01/opencti-inteligencia-ciberamenazas/>
- San José, J. (2022b). *Osintgram, una herramienta OSINT para Instagram*. Recuperado de <https://derechodelared.com/2022/07/03/osintgram-osint-instagram/>
- Sánchez, G. (2024). *Orquestando la Incertidumbre en Seguridad: Hipótesis, Inteligencia y el Baile de las Probabilidades*. Recuperado de <https://es.linkedin.com/pulse/orquestando-la-incertidumbre-en-seguridad-hip%C3%B3tesis-y-germ%C3%A1n-8shuc>
- SANS Institute. (2009). *Security Intelligence: Attacking the Cyber Kill Chain*. Recuperado de <https://www.sans.org/blog/security-intelligence-attacking-the-cyber-kill-chain>
- SANS Institute. (2021). *BloodHound – Sniffing Out the Path Through Windows Domains*. Recuperado de <https://www.sans.org/blog/bloodhound-sniffing-out-path-through-windows-domains>
- SC Media. (2024). *NATO, others targeted by novel hacktivist collective*. Recuperado de <https://www.scworld.com/brief/nato-others-targeted-by-novel-hacktivist-collective>
- Schmitt, M. N. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press.
- Seaton, D. (2024). *Understanding the Web: Dark Web, Deep Web, and Clear Web*. Recuperado de <https://cyberauditteam.com/blog/understanding-the-dark-web>
- Securityaffairs. (2017). *Nato presents the Tallinn Manual 2.0 on international law applicable to cyberspace*. Recuperado de <https://securityaffairs.com/56004/cyber-warfare-2/nato-tallinn-manual-2-0.html>
- Seisdedos, C. (2023). *Virtual HUMINT y consejos para ciberinvestigar de forma segura*. Recuperado de <https://www.lisanews.org/ciberseguridad/virtual-humint-y-consejos-para-ciberinvestigar/>
- Severiche, L. (2022). *Monitorización de la reputación electrónica: Cómo analizar la reputación de tu marca con los KPIs correctos*. Recuperado de <https://blog.digimind.com/es/insight-driven-marketing/monitorizacion-ereputacion-electronica-analizar-reputacion-marca-kpi-correctos>

- Sharma, M. (2025). *Bug Hunting Recon Guide: Find Hidden Vulnerabilities Like a Pro*. Recuperado de <https://osintteam.blog/bug-hunting-recon-guide-find-hidden-vulnerabilities-like-a-pro-353accfe65c4>
- Simpere, E. (2024). *Kill Chain: infórmese para protegerse mejor*. Recuperado de <https://www.stormshield.com/es/noticias/kill-chain-informese-para-protegerse-mejor/>
- Slack. (2023). *Virtual hosts: qué son y cómo funcionan*. Recuperado de <https://slack.com/intl/es-es/blog/transformation/virtual-hosts-que-son-y-como-funcionan>
- SOCRadar. (2024). *Dark Web Profile: Cyber Army of Russia Reborn*. Recuperado de <https://socradar.io/dark-web-profile-cyber-army-of-russia-reborn/>
- Soto, J. (2020). *¿Qué es Instagram y para qué sirve?* Recuperado de <https://www.geeknetic.es/Instagram/que-es-y-para-que-sirve>
- StrangeBee. (s.f.). *TheHive. Collaborative Case Management Platform for cybersecurity teams*. Recuperado de <https://strangebee.com/thehive/>
- Suárez, A. (2019). *Diferencias entre Surface web, Deep web y Dark web*. Recuperado de <https://www.a2secure.com/blog/diferencias-entre-surface-web-deep-web-y-dark-web/>
- Suárez, P. (2024). *Qué es Facebook, cómo funciona y para qué sirve en marketing*. Recuperado de <https://www.seonetdigital.com/es/blog/que-es-facebook>
- Tannhausser. (2012). *Freenet: una red del internet underground*. Recuperado de <https://lamiradadelreplicante.com/2012/11/20/freenet-una-red-del-internet-underground/>
- Taysir, S. (2021). *Vkontakte, la red social rusa*. Recuperado de <https://altraducciones.com/blog/vkontakte-red-social-rusa>
- Terkait, B. (2024). *Recorded Future Highlights Alarming Shift in Hacktivism Trends*. Recuperado de <https://si.ft.unesa.ac.id/post/recorded-future-highlights-alarming-shift-in-hacktivism-trends>
- TGStat. (s.f.). *NoName057(16) Eng*. Recuperado de <https://tgstat.com/channel/@noname05716eng>
- Thee Eclipse. (2023). *Bug Bounty Recon Guide*. Recuperado de <https://infosecwriteups.com/bug-bounty-manual-recon-guide-57e1e5a06dd7>
- Tidmarsh, D. (2023). *Diamond Model of Intrusion Analysis: What, Why, and How to Learn*. Recuperado de <https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/diamond-model-intrusion-analysis/>
- Tilborghs, S. & Jarosz, K. (2023). *La palabra clave más común de combosquatting es "support"*. Recuperado de <https://www.akamai.com/es/blog/security-research/combosquatting-keyword-analysis-support>
- Trend Micro. (2025). *¿Qué es la Gestión de la Exposición?* Recuperado de https://www.trendmicro.com/es_es/what-is/attack-surface/exposure-management.html
- Tripledobleu. (2021). *¿Qué es un registro CVE?* Recuperado de <https://tripledoubleu.online/que-es-un-registro-cve/>
- Twingate Team. (2024). *What is Wardriving?* Recuperado de <https://www.twingate.com/blog/glossary/wardriving>
- UNIR. (2021). *¿Qué es el hacktivismo y qué delitos implica?* Recuperado de <https://www.unir.net/revista/derecho/hacktivism/>
- U-Tad. (2023). *¿Qué es el Hacktivismo?* Recuperado de <https://u-tad.com/hacktivism/>

- Véliz, D. (2021). *Qué es Vkontakte (VK): la versión rusa de Facebook que ahora está en manos de su gobierno*. Recuperado de <https://marketing4ecommerce.net/la-red-social-rusa-vkontakte/>
- Wegener, H. (2013). *Los riesgos económicos de la ciberguerra*. Instituto Español de Estudios Estratégicos. Recuperado de <https://dialnet.unirioja.es/servlet/articulo?codigo=4276097>
- Wenzler, N. (2022). *Gestión de exposición: reducción del riesgo en la superficie de ataque moderna*. Recuperado de <https://es-la.tenable.com/blog/exposure-management-reducing-risk-in-the-modern-attack-surface>
- Yubal, F. (2016). *Así es Freenet, deep web alternativa a Tor e I2P*. Recuperado de <https://www.genbeta.com/a-fondo/asi-es-freenet-deep-web-alternativa-a-tor-e-i2p>
- Zafra, L.A. (2025). *Más Allá de las Alertas: Fortalece tu Ciberdefensa con Feeds de CTI, el Ciclo de Vida y OTX*. Recuperado de <https://www.linkedin.com/pulse/m%C3%A1s-all%C3%A1-de-las-alertas-fortalece-tu-ciberdefensa-con-zafra-labrador-ezqyc>