Arquitectura de *Cyber Situational Awareness* para la protección de infraestructuras críticas

Departamento de Comunicaciones
Universitat Politècnica de València

Tesis presentada para la obtención del grado de
Doctor por la Universitat Politècnica de València
Valencia, Diciembre de 2018

Autor:
Javier Hingant Gómez

Director:
Dr. Manuel Esteve Domingo

A Amanda,

con quien el viaje siempre será más bonito.

Resumen

La seguridad en el ciberespacio supone hoy en día un reto fundamental para cualquier organización ante el incesante aumento de ciberataques en todo el mundo. En una realidad tecnológica como la actual, en la que los dominios físico y lógico son cada vez más interdependientes, esta tarea es todavía más imprescindible pues las acciones en cualquiera de estos ámbitos pueden acarrear consecuencias devastadoras en ambos. Esto es si cabe más importante en el caso de infraestructuras críticas (IC), pues de su correcto funcionamiento depende el bienestar de toda una nación y sus ciudadanos.

Se hacen por tanto necesarias nuevas soluciones que permitan afrontar de manera eficiente la defensa de toda clase de IC en este escenario híbrido, en el que las herramientas tradicionales de seguridad (*firewall*, IDS/IPS e incluso sistemas SIEM) resultan por sí solas insuficientes ante ataques a gran escala y donde alternativas más completas como los sistemas SCADA más recientes siguen orientadas a sectores muy específicos.

La presente tesis doctoral plantea un enfoque innovador de *Situational Awareness* (SA) para la adecuada protección de IC en el contexto ciber-físico. En concreto, se propone una arquitectura genérica de SA híbrida que proporcione, mediante técnicas avanzadas de representación, la *Common Operational Picture* conjunta de las dimensiones física y ciber en un espacio único de visualización con el fin de facilitar la toma de decisiones al operador correspondiente.

La arquitectura definida ha sido aplicada en dos soluciones distintas de *Cyber Command & Control* para la protección de IC: el sistema GESTPIC para la visualización avanzada de la SA ciber-física, y HYBINT como novedosa herramienta para la integración y el análisis de información de inteligencia.

El modelo presentado en esta investigación ha sido validado en entornos de uso tanto simulados como reales, suscitando el interés de potenciales usuarios finales y confirmándose como propuesta pionera en su campo en los foros especializados en los que ha participado.

RESUMEN

Resum

La seguretat en el ciberespai suposa hui dia un repte fonamental per a qualsevol organització davant l'incessant augment de ciberatacs a tot el món. En una realitat tecnològica com l'actual, en la qual els dominis físic i lògic són cada vegada més interdependents, aquesta tasca és encara més imprescindible perquè les accions en qualsevol d'aquests àmbits poden implicar conseqüències devastadores en tots dos. Això és si cap més important en el cas d'infraestructures crítiques (IC), perquè del seu correcte funcionament depén el benestar de tota una nació i els seus ciutadans.

Es fan per tant necessàries noves solucions que permeten afrontar de manera eficient la defensa de tota classe d'IC en aquest escenari híbrid, en el qual les eines tradicionals de seguretat (*firewall*, IDS/IPS i fins i tot sistemes SIEM) resulten per si soles insuficients davant atacs a gran escala i on alternatives més completes com els sistemes SCADA més recents segueixen orientades a sectors molt específics.

La present tesi doctoral planteja un enfocament innovador de *Situational Awareness* (SA) per a l'adequada protecció d'IC en el context ciber-físic. En concret, es proposa una arquitectura genèrica de SA híbrida que proporcione, mitjançant tècniques avançades de representació, la *Common Operational Picture* conjunta de les dimensions física i ciber en un espai únic de visualització amb la finalitat de facilitar la presa de decisions a l'operador corresponent.

L'arquitectura definida ha sigut aplicada en dues solucions diferents de *Cyber Command & Control* per a la protecció d'IC: el sistema GESTPIC per a la visualització avançada de la SA ciber-física, i HYBINT com a nova eina per a la integració i l'anàlisi d'informació d'intel·ligència.

El model presentat en aquesta investigació ha sigut validat en entorns d'ús tant simulats com reals, suscitant l'interés de potencials usuaris finals i confirmant-se com a proposta pionera en el seu camp en els fòrums especialitzats en els quals ha participat.

Abstract

Security in cyberspace is today a key challenge for any organization with the continuous growth of cyberattacks worldwide. In the current technological reality, in which physical and cyber domains are increasingly interdependent, this task is still most essential since actions in any of these scopes can lead to devastating consequences on both. This is even more important in case of critical infrastructures (CI), inasmuch as well-being of nations and their citizens depends on their proper functioning.

New solutions are therefore needed in order to efficiently face the defence of all kind of CI in this hybrid scenario, in which traditional security tools (firewall, IDS/IPS and even SIEM systems) are by themselves insufficient against large-scale attacks and where more complete workarounds such as the most recent SCADA systems still remain focused on very specific sectors.

This doctoral thesis introduces an innovative Situational Awareness (SA) approach for the suitable CI protection in the cyber-physical context. In particular, a hybrid SA architecture that provides, through advanced representation techniques, a Common Operational Picture of both physical and cyber dimensions in a unique visualization space is proposed to support operator's decision-making.

The defined architecture has been applied in two different Cyber Command & Control solutions for CI protection: GESTPIC system for cyber-physical SA advanced visualization, and HYBINT as a novel tool for intelligence information integration and analysis.

The model presented in this research has been validated in both simulated and real working environments, awakening the interest of potential end users and being confirmed as a ground-breaking proposal in its field in the specialized forums in which it has participated.

ABSTRACT

Agradecimientos

En primer lugar, mi más sincero y profundo agradecimiento a mi director, Dr. D. Manuel Esteve Domingo, no solo por brindarme esta oportunidad única sino también por apostar decididamente por mí, hace ya unos cuantos años, y descubrirme una profesión que me estimula y realiza a partes iguales.

De igual modo, a todos y cada uno de mis compañeros del grupo de investigación de SATRD, sin quienes no habría sido posible esta aventura, por su incuestionable apoyo y su predisposición a seguir creciendo juntos día a día.

Como no, a esa gran familia que uno elige, colegas y amigos de aquí y de allá a quienes tanto debo, por ser mi válvula de escape y mi eterno refugio, por incontables batallas a cuestas y sin embargo tantas páginas aun por escribir.

Desde luego y con especial cariño, a los que han estado ahí desde el principio, a mi familia. A mi madre Lola, la mejor de las maestras y mi principal referente, por contagiarme su encomiable sentido de la dedicación y transmitirme el valor del esfuerzo. A mi hermano Alex, a menudo tan lejos pero siempre tan presente, por alentarme a cada paso y enseñarme a nunca perder la ilusión.

Por último y sin duda alguna, a mi razón de superación constante, mi compañera en la vida y a la vez mi mayor confidente. A Amanda, por todo y por tanto, por invitarme a soñar cada día, por su inmensa paciencia, su infinita confianza y su amor incondicional.

Muchas gracias a todos.

Javier Hingant Gómez
Valencia, Diciembre de 2018

AGRADECIMIENTOS

Índice

Índice de figuras xiii

Índice de tablas xv

Acrónimos xvii

1. Introducción 1
- 1.1. Introducción . . . 1
- 1.2. Motivaciones . . . 5
- 1.3. Objetivos de la tesis . . . 7
- 1.4. Principales aportaciones . . . 8
  - 1.4.1. Artículos . . . 8
  - 1.4.2. Congresos y Jornadas . . . 8
  - 1.4.3. Proyectos de investigación . . . 8
  - 1.4.4. Desarrollo software . . . 9
- 1.5. Organización de la memoria . . . 9

2. Estado del arte 11
- 2.1. Introducción . . . 11
- 2.2. Situación en el ciberespacio . . . 14
  - 2.2.1. Tipos de ciberataque . . . 15
  - 2.2.2. Agentes de la amenaza . . . 20
  - 2.2.3. Víctimas y consecuencias . . . 22
  - 2.2.4. Principales vulnerabilidades . . . 24
- 2.3. Infraestructuras críticas . . . 26
  - 2.3.1. Definición de infraestructura crítica . . . 26
  - 2.3.2. Clasificación de infraestructuras críticas . . . 27
  - 2.3.3. Interdependencia de infraestructuras críticas . . . 29
- 2.4. *Cyber Situational Awareness* . . . 32
  - 2.4.1. Marco general . . . 32

2.4.2. Sensores y fuentes de datos 38
2.4.3. Métodos y herramientas de análisis 42
2.4.4. Técnicas de visualización de información 48

3. Definición de la arquitectura 59
3.1. Introducción 59
3.2. Visión general 60
3.3. Adquisición de datos 61
3.3.1. Fuentes de datos ciber 61
3.3.2. Fuentes de datos físicos 64
3.3.3. Fuentes de datos mixtos 64
3.3.4. Interoperabilidad 65
3.4. Fusión de datos 69
3.4.1. Modelo relacional 69
3.4.2. Base de datos 71
3.5. Análisis de datos 72
3.5.1. Análisis de riesgos 72
3.5.2. Análisis de inteligencia 75
3.6. Representación de información 76
3.6.1. Información geolocalizada 77
3.6.2. Diagramas y grafos 78
3.6.3. Visualización inmersiva 79

4. Validación de la arquitectura: GESTPIC 81
4.1. Introducción 81
4.2. Motivación y objetivos 82
4.2.1. Características principales 83
4.2.2. Casos de uso 83
4.3. Arquitectura del sistema 86
4.3.1. Módulo de interoperabilidad 89
4.3.2. Módulo de acceso a BBDD 90
4.3.3. Módulo de análisis y correlación 91
4.3.4. Módulo de GIS 94
4.3.5. Módulo de generación de visualizaciones 94
4.3.6. Módulo de visualización inmersiva 96
4.3.7. Módulo HMI 97

5. Evaluación del sistema GESTPIC 99
5.1. Introducción 99
5.2. Evaluación de GESTPIC 100
5.2.1. Especificaciones técnicas 100

5.2.2. Escenario de pruebas 102
5.2.3. Evaluación de la solución 103
5.3. Participación en proyecto SAURON 107

6. Validación de la arquitectura: HYBINT **111**
6.1. Introducción 111
6.2. Antecedentes y objetivos 112
6.3. Arquitectura del sistema 114
6.3.1. Módulo de adquisición de datos 116
6.3.2. Módulo de análisis de datos 118
6.3.3. Módulo de visualización de datos 120
6.3.4. Características adicionales 122

7. Conclusiones **125**
7.1. Conclusiones finales 125
7.1.1. Conclusiones generales 125
7.1.2. Sistema GESTPIC 128
7.1.3. Sistema HYBINT 129
7.2. Líneas futuras de investigación 130

Referencias **133**

Índice de figuras

1.1. Interacción de dominios físico y ciber 1
1.2. Incidentes contra sectores críticos: un problema global 2
1.3. Incidentes en infraestructuras críticas de EEUU (2012-2015) . . 3
1.4. Incidentes gestionados por el CCN-CERT (2009-2016) 4
1.5. Costes de recuperación según tiempo hasta detección 4

2.1. Vista tradicional de Mando y Control: bucle OODA 12
2.2. Modelo de *Situational Awareness* en tres niveles 13
2.3. Tasa de incidencia de *ransomware* (abril-junio de 2016) 15
2.4. Incidencia de ataques DDoS (octubre de 2016) 17
2.5. Ataques a aplicaciones web (octubre-diciembre de 2016) 18
2.6. Incidentes sufridos por ciudadanos españoles 23
2.7. Grado de ciberconcienciación de ciudadanos europeos 26
2.8. Tipos de ataque por sectores críticos 30
2.9. Interdependencia de infraestructuras críticas (Rinaldi *et al.*) . . 31
2.10. Modelo genérico de CySA en cinco fases (Matthews *et al.*) . . . 33
2.11. Interfaz de visualización de CySA (Klein *et al.*) 36
2.12. *Cyber Kill Chain* 38
2.13. Funcionamiento genérico de un SIEM 39
2.14. Gestión de riesgos (ISO 31000:2009) 47
2.15. Técnicas de georreferenciación de la información 53
2.16. Grafos y diagramas interactivos 54
2.17. Representaciones tridimensionales de datos complejos 55
2.18. Ejemplos de visualización inmersiva 57

3.1. Visión general de la arquitectura 60
3.2. Vista de la interfaz de OSSIM 62
3.3. Vista de la interfaz de MISP 62
3.4. Vista de la interfaz de RTIR 63

3.5. Ejemplo de API web AlienVault 66
3.6. Ejemplo de API web MISP 67
3.7. Ejemplo de API web RTIR 67
3.8. Ejemplo de petición NVG 68
3.9. Mecanismos de comunicación 69
3.10. Modelo de datos simplificado 70
3.11. Proceso de análisis de riesgos (metodología MAGERIT) 73

4.1. Sistemas y actores de GESTPIC 84
4.2. Arquitectura del sistema 87
4.3. Vista principal de GESTPIC 88
4.4. Módulo de interoperabilidad 89
4.5. Configuración de fuentes externas 90
4.6. Módulo de acceso a BBDD 90
4.7. Módulo de análisis y correlación 91
4.8. Estado de activos físicos y ciber 92
4.9. Análisis de riesgos y de consecuencias 93
4.10. Módulo de GIS 94
4.11. Módulo de generación de visualizaciones 94
4.12. Grafos 3D georreferenciados 95
4.13. Otras representaciones 95
4.14. Módulo de visualización inmersiva 96
4.15. Visualización inmersiva 97
4.16. Módulo HMI 97

5.1. Entorno virtualizado de pruebas 103
5.2. Concepto general de SAURON 108

6.1. Instalaciones del C-IED CoE (Hoyo de Manzanares, Madrid) . 112
6.2. Arquitectura del sistema 115
6.3. Módulo de adquisición de datos (DGM) 117
6.4. Módulo de análisis de datos (DAM) 119
6.5. Ejemplos de uso de IBM i2 Analyst's Notebook 120
6.6. Módulo de visualización de datos (DVM) 121

Índice de tablas

2.1. Atacantes y sus principales motivaciones 22
2.2. Principales costes derivados de ciberincidentes 24
2.3. Clasificación de infraestructuras críticas 29
2.4. Sectores críticos adicionales 29
2.5. Capacidades de visualización e interacción (Klein *et al.*) 37
2.6. Tipos de dispositivos de VR y sus características 56

3.1. Fuentes de datos de la arquitectura de HSA 65
3.2. Bases de datos SQL y NoSQL 71
3.3. Principales grafos y diagramas 79

4.1. Casos de uso de GESTPIC 86

5.1. Especificaciones técnicas de Oculus Rift 100
5.2. Especificaciones técnicas de NVIDIA GeForce GTX 970 101
5.3. Requisitos mínimos de hardware 101
5.4. Requisitos mínimos de hardware sin VR 102
5.5. Pruebas de evaluación técnica del sistema 105
5.6. Pruebas de evaluación operativa del sistema 106

6.1. Niveles de acceso al sistema y capacidades asociadas 123

ÍNDICE DE TABLAS

Acrónimos

API	*Application Programming Interface*
AR	*Augmented Reality*
C-IED CoE	*Counter-Improvised Explosive Devices Centre of Excellence*
C2	*Command & Control*
C4ISR	*Command, Control, Communications, Computers, Intelligence, Surveillance & Reconnaissance*
CCN-CERT	Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional
CIUSAT	*C-IED Interagency Unclassified Situational Awareness Tool*
COP	*Common Operational Picture*
CPS	*Cyber Physical Systems*
CySA	*Cyber Situational Awareness*
DAM	*Data Analysis Module*
DDoS	*Distributed Denial of Service*
DGM	*Data Gathering Module*
DHS	*Department of Homeland Security*
DoD	*Department of Defense*
DoS	*Denial of Service*
DVM	*Data Visualization Module*

ACRÓNIMOS

ENISA	*European Union Agency for Network and Information Security*
EPCIP	*European Programme for Critical Infrastructure Protection*
ESM	*Enterprise Security Manager*
ESRI	*Environmental Systems Research Institute*
GESTPIC	Gestión y Protección de Infraestructuras Críticas
GIS	*Geographic Information System*
H2020	*Horizon 2020 Programme*
HMD	*Head-Mounted Displays*
HMI	*Human-Machine Interface*
HSA	*Hybrid Situational Awareness*
HTTP	*Hypertext Transfer Protocol*
HUMINT	*Human Intelligence*
HYBINT	*Hybrid Intelligence*
ICS	*Industrial Control Systems*
IDS	*Intrusion Detection System*
IIS	*Internet Information Services*
IoT	*Internet of Things*
IPS	*Intrusion Prevention System*
JSON	*JavaScript Object Notation*
KML	*Keyhole Markup Language*
LUCIA	Listado Unificado de Coordinación de Incidentes y Amenazas
MAGERIT	Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información
MISP	*Malware Information Sharing Platform and Threat Sharing*

NIST	*National Institute of Standards and Technology*
NVG	*NATO Vector Graphics*
OGC	*Open Geospatial Consortium*
OODA	*Observe, Orient, Decide and Act*
OSINT	*Open Source Intelligence*
OSSIM	*Open Source Security Information Management*
OTAN	Organización del Tratado del Atlántico Norte
OTX	*Open Threat Exchange*
PILAR	Procedimiento Informático-Lógico para el Análisis de Riesgos
PSA	*Physical Situational Awareness*
PyMEs	Pequeñas y Medianas Empresas
REST	*REpresentational State Transfer*
RT	*Request Tracker*
RTIR	*Request Tracker for Incident Response*
SA	*Situational Awareness*
SAGAT	*Situation Awareness Global Assessment Technique*
SATRD	Sistemas y Aplicaciones de Tiempo Real Distribuidos
SAURON	*Scalable multidimensionAl sitUation awaReness sOlution for protectiNg european ports*
SCADA	*Supervisory Control And Data Acquisition*
SCAP	*Security Content Automation Protocol*
SDK	*Software Development Kit*
SIEM	*Security Information and Event Management*
SQL	*Structured Query Language*
STIX	*Structured Threat Information eXpression*

ACRÓNIMOS

SVG	*Scalable Vector Graphics*
TIC	Tecnologías de la Información y la Comunicación
USM	*Unified Security Management*
UTM	*Unified Threat Management*
VR	*Virtual Reality*
XML	*eXtensible Markup Language*

Capítulo 1

Introducción

1.1. Introducción

En los últimos años, el acelerado desarrollo de la tecnología ha incidido en todos los sectores de la sociedad permitiendo a las organizaciones incrementar la eficiencia de sus actividades al expandir su ámbito de operaciones al ciberespacio y esquivar, de este modo, algunas de las limitaciones asociadas al mundo físico tales como los mercados o las fronteras [1][2].

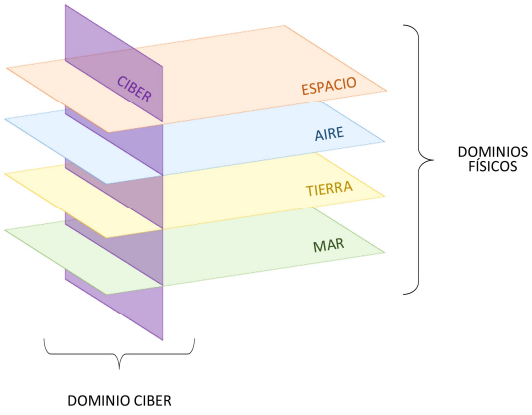


Figura 1.1: Interacción de dominios físico y ciber.

Las Tecnologías de la Información y la Comunicación (TIC) [3] lideran sin lugar a dudas esta reciente transformación donde, áreas de investigación actuales como el *Big Data* [4], tecnologías basadas en la nube [5][6], la inteligencia artificial [7] o el internet de las cosas (*Internet of Things* (IoT)) [8] encabezan un nuevo paradigma en el que el espacio ciber viene a integrarse con todas y cada una de las dimensiones del mundo físico (tierra, mar, aire y espacio) dando lugar a un entorno híbrido (o mixto) donde entidades físicas y ciber ya no pueden entenderse de manera independiente (Figura 1.1) [9].

Este entorno ciber-físico [10] ofrece un amplio conjunto de oportunidades pero a la vez nuevas vulnerabilidades y riesgos que deben ser adecuadamente gestionadas. En efecto, más allá de las clásicas amenazas relativas al mundo físico, organizaciones en general e infraestructuras críticas en particular, deben ahora hacer frente también a todas aquellas existentes en el ciberespacio [11]. Dicha tarea resulta todavía más compleja debido a los llamados "efectos cascada", es decir, a las implicaciones en cadena sobre los mundos físico y ciber causadas por ataques provenientes de cualquiera de ellos.

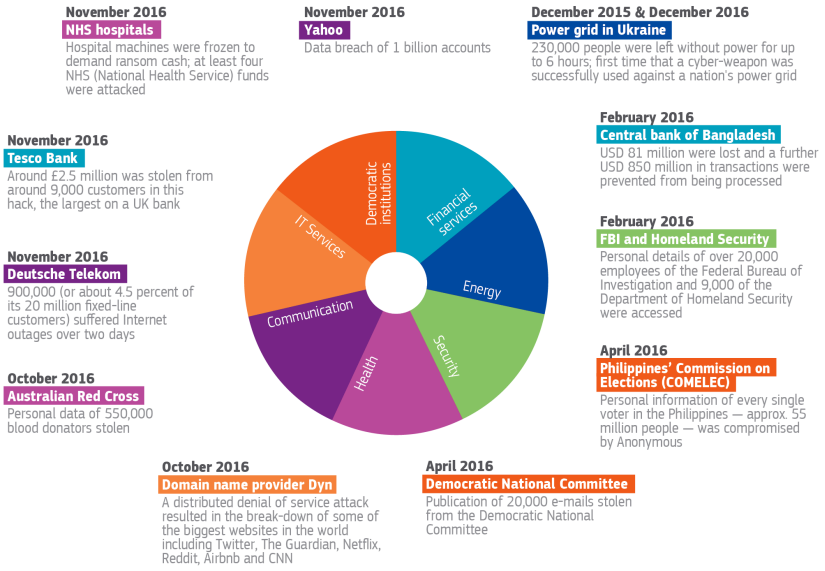


Figura 1.2: Incidentes contra sectores críticos: un problema global [1].

[1] European Political Strategy Centre (EPSC), "Building an Effective European Cyber Shield: Taking EU Cooperation to the Next Level," *EPSC Strategic Notes*, no. 24, May 2017.

El crecimiento exponencial de los ciberataques, tanto a pequeña como a gran escala, en la última década es responsable de incalculables pérdidas y daños a lo largo y ancho del planeta. Tal y como confirma la Figura 1.2, extraída de un estudio del *European Political Strategy Centre* (EPSC) [12] y donde únicamente constan algunos de los principales ciber incidentes acontecidos a lo largo del año 2016, se trata de una problemática a escala global a la que no escapa ninguno de los considerados como sectores críticos [13].

La Figura 1.3 ilustra el crecimiento de los ciber incidentes reportados por el *Department of Homeland Security* (DHS) de los Estados Unidos [14] en los últimos años contra infraestructuras críticas norteamericanas. Entre estos, cabe destacar campañas *ransomware* como *Petya* [15] o *Wannacry* [16], la cual pudo afectar a más de 15 millones de equipos de más de 10.000 organizaciones causando unas pérdidas económicas que se aproximaron a los 200 millones de euros [17].

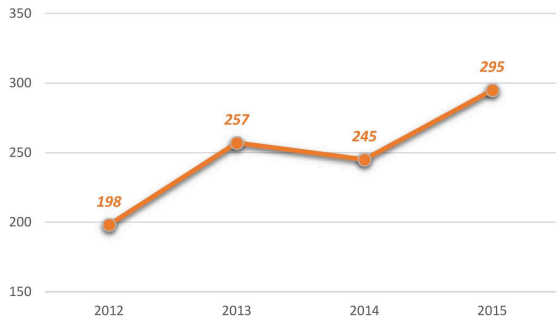


Figura 1.3: Incidentes en infraestructuras críticas de EEUU (2012-2015) [2].

Misma tendencia se observa en España (Figura 1.4) donde la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional (CCN-CERT) [18], adscrito al Centro Nacional de Inteligencia (CNI) [19] y responsable de los ciber incidentes que afecten a cualquier organismo o empresa pública nacional, gestionó solo en el año 2016 casi 21.000 incidentes, lo que representa un 15 % más respecto al año anterior (18.232) y un incremento del 424 % en tan solo 5 años (en 2012, 3.998) [20][21].

Cabe destacar el caso de Estonia, convertida hoy día en referente mundial gracias a las tecnologías en ciberseguridad desarrolladas a raíz del ciberataque sufrido en el año 2007, el cual trasladó el país a la Edad de Piedra dejando en blanco todos los sitios web gubernamentales [22].

[2] Department of Homeland Security (DHS), `https://www.dhs.gov` [Accessed May 8, 2018].

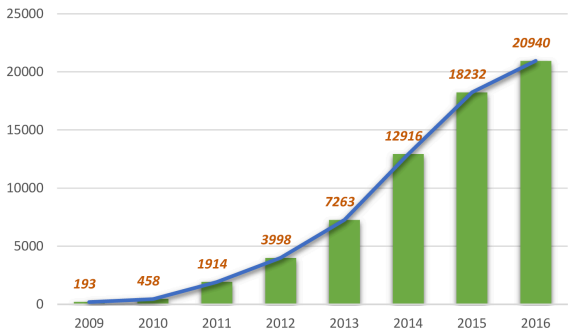


Figura 1.4: Incidentes gestionados por el CCN-CERT (2009-2016) [3].

La rápida respuesta de los sistemas de seguridad resulta un factor crítico a la hora de minimizar los daños producidos por un ciber ataque. Así lo demuestra un estudio realizado por Kaspersky Lab. [23] en 2016 a más de 4.000 empresas de 25 países diferentes [24] (Figura 1.5).

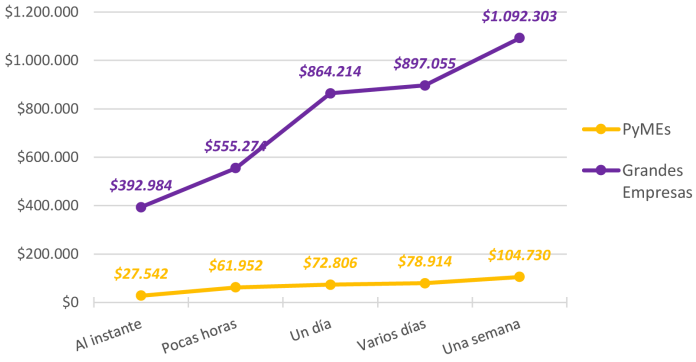


Figura 1.5: Costes de recuperación según tiempo hasta detección [4].

Como puede verse, los costes económicos de recuperación aumentan notablemente con el tiempo transcurrido desde que se produce un incidente hasta

[3] Centro Criptológico Nacional (CCN-CERT), "Ciberamenazas y Tendencias - Resumen Ejecutivo," CCN-CERT, Madrid, Spain, IA-09/16, 2016.

[4] Kaspersky Lab, "Measuring Financial Impact of IT Security on Businesses," *IT Security Risks Report Series*, 2016.

que es detectado. Estos son todavía mayores cuando se trata de grandes empresas o multinacionales.

Con el fin de garantizar una defensa eficiente en este escenario híbrido, en el que riesgos y amenazas han adquirido una nueva dimensión, se imponen nuevas estrategias, herramientas de seguridad y planes de acción que satisfagan las exigencias del entorno actual [25]. Estos requerimientos resultan aún más si cabe imprescindibles en la protección a infraestructuras críticas, cuyo mantenimiento y buen funcionamiento son imprescindibles para la seguridad y el bienestar de cualquier país [26].

Sin embargo, pese a que existen alternativas bajo la forma de sistemas de *Physical Situational Awareness* (PSA) o *Cyber Situational Awareness* (CySA) para la protección de organizaciones e infraestructuras frente a amenazas de origen físico o ciber respectivamente, resulta difícil encontrar soluciones reales basadas en una *Situational Awareness* (SA) mixta, es decir, que consideren la situación del entorno ciber-físico en su conjunto en un único espacio de actuación. En efecto, la mayoría de las propuestas examinadas en esta línea o bien consisten en modelos teóricos todavía sin implementar o bien están enfocadas a la defensa de un determinado tipo de organización en particular.

Es por tanto objeto de la presente tesis doctoral el diseño de una arquitectura genérica de SA híbrida, o *Hybrid Situational Awareness* (HSA), que mejore el proceso de toma de decisiones para la protección de cualquier tipo de infraestructura crítica en el espacio ciber-físico así como su aplicación a dos soluciones distintas en el ámbito del *Cyber Command & Control*:

- **GESTPIC**: sistema avanzado de visualización de HSA que fusiona, en un único espacio de toma de decisiones, la situación en tiempo real de los dominios físico y ciber.
- **HYBINT**: sistema de inteligencia híbrida que combina información tanto de sistemas físicos y ciber como de fuentes humanas o abiertas para una mayor HSA del entorno.

1.2. Motivaciones

La investigación, tanto teórica como aplicada, desarrollada a lo largo de esta tesis doctoral ha estado orientada a dos casos de aplicación de CySA. Se ha hecho por tanto necesaria la definición de sendas arquitecturas específicas para la protección de infraestructuras críticas de acuerdo con los requisitos y necesidades de cada uno de estos escenarios de uso.

A continuación, se exponen las principales motivaciones conducentes a la realización de la presente tesis doctoral:

- **Consciencia conjunta de la situación**

  En la actualidad, existen diversas soluciones para la protección de infraestructuras críticas consistentes en sistemas de SA orientados exclusivamente al entorno físico o al entorno ciber.

  Sin embargo, en un contexto como el actual en el que ambos dominios ya no pueden entenderse de manera independiente, se hacen necesarias herramientas más avanzadas que ofrezcan una consciencia situacional del entorno ciber-físico (o híbrido) en su conjunto al integrar, en un único espacio para la toma de decisiones, la situación en tiempo real de cada una de estas dimensiones.

- **Especificación de arquitectura flexible**

  Se considera fundamental el diseño de una arquitectura genérica que resulte fácilmente adaptable a los requisitos y necesidades asociados a cada uno de sus casos de uso y que permita la integración de nuevas herramientas y funcionalidades en el futuro.

- **Fuentes heterogéneas de datos**

  La arquitectura a implementar ha de ser capaz de adquirir información procedente de fuentes heterogéneas de datos, de los ámbitos tanto físico como ciber, que responden a modelos de datos dispares y almacenarla siguiendo un esquema único de base de datos.

- **Usabilidad de las aplicaciones**

  Las soluciones existentes que han sido estudiadas se presentan excesivamente complejas o poco intuitivas para el usuario. Resulta por tanto prioritario que el desarrollo de las aplicaciones esté basado en módulos simples y desacoplados que potencien la facilidad de uso de las mismas.

- **Técnicas avanzadas de visualización**

  Novedosas técnicas de representación de la información han aparecido en los últimos años cuya utilización conlleva una notable mejora en la percepción de la situación. La integración de algunas de ellas es uno de los principales objetivos de Gestión y Protección de Infraestructuras Críticas (GESTPIC) y supone un valor añadido respecto a soluciones existentes en su ámbito.

- **Inteligencia híbrida**

  Las herramientas tradicionales de inteligencia están habitualmente centradas en el tratamiento de información adquirida por medios humanos.

Hybrid Intelligence (HYBINT) pretende constituirse en un sistema de inteligencia híbrida que incorpore tanto fuentes de información adicionales como capacidades avanzadas de análisis a una herramienta preexistente de *Human Intelligence* (HUMINT).

1.3. Objetivos de la tesis

A partir de las motivaciones expuestas en el apartado anterior, se han definido los siguientes como objetivos principales de la presente tesis doctoral:

- Analizar el estado del arte en CySA y reseñar algunas de las propuestas más destacables encaminadas a su adecuada representación.
- Exponer la situación actual en el ciberespacio y argumentar la necesaria protección eficiente de las infraestructuras críticas en el entorno híbrido.
- Definir una arquitectura genérica para la visualización de HSA siguiendo las características expuestas en la presente tesis y de acuerdo con los requisitos de uso de cada uno de los sistemas a implementar.
- Estudiar e integrar las más novedosas técnicas de representación para la visualización avanzada de la información ciber-física en un espacio único de toma de decisiones.
- Desarrollar módulos de interoperabilidad para la comunicación con fuentes heterogéneas de datos de los dominios tanto físico como ciber.
- Especificar capacidades de análisis y correlación de datos en el marco del análisis y evaluación de riesgos en GESTPIC y para la generación de información avanzada de inteligencia en HYBINT.
- Aplicar el modelo planteado al diseño del sistema GESTPIC como solución innovadora para la visualización conjunta de la SA física y ciber que facilite la adecuada protección de infraestructuras críticas.
- Aplicar el modelo planteado al diseño del sistema HYBINT como propuesta de una solución avanzada para la integración y el análisis de información de inteligencia de fuentes diversas.
- Evaluar técnica y operativamente un prototipo final del sistema GESTPIC en escenarios de uso tanto simulados como reales.

1.4. Principales aportaciones

1.4.1. Artículos

- **J. Hingant**, M. Zambrano, F. Pérez, I. Pérez, and M. Esteve, "HYBINT: A Hybrid Intelligence System for Critical Infrastructures Protection," *Security and Communication Networks*, vol. 2018, pp. 1–13, Aug. 2018.

1.4.2. Congresos y Jornadas

- M. Esteve, I. Pérez, C. E. Palau, F. Carvajal, and **J. Hingant**, "Cyber Common Operational Picture: A Tool for Cyber Hybrid Situational Awareness Improvement," in *STO Symposium on Cyber Defence Situation Awareness (STO-MP-IST-148)*, Sofia, Bulgaria, Oct. 3-4, 2016, pp. 1-10.

- **J. Hingant**, "Ciberseguridad para infraestructuras críticas: Una solución basada en *Hybrid Situational Awareness* (HSA)," in *VII Jornadas Doctorales de la Universidad de Castilla-La Mancha*, Albacete, Spain, Nov. 7, 2017.

- S. Llopis, **J. Hingant**, I. Pérez, M. Esteve, F. Carvajal, W. Mees, and T. Debatty, "A comparative analysis of visualisation techniques to achieve cyber situational awareness in the military," in *2018 International Conference on Military Communications and Information Systems (ICMCIS)*, Warsaw, Poland, May 22-23, 2018, pp. 1-7.

- **J. Hingant**, and M. Esteve, "GESTPIC: An Advanced and Innovative Cyber-Physical System (CPS) for Critical Infrastructures Protection," in *18th IEEE International Conference on Software Quality, Reliability, and Security (QRS)*, Lisbon, Portugal, Jul. 16-20, 2018.

- S. Schauer, B. Rainer, N. Museux, D. Faure, **J. Hingant**, F. Carvajal, S. Beyer, R. Company, and S. Zamarripa, "Conceptual Framework for Hybrid Situational Awareness in Critical Port Infrastructures," in *13th International Conference on Critical Information Infrastructures Security (CRITIS)*, Kaunas, Lithuania, Sep. 24-26, 2018, pp. 191-203.

1.4.3. Proyectos de investigación

- Proyectos *C-IED Interagency Unclassified Situational Awareness Tool* (CIUSAT) y Gestión y Protección de Infraestructuras Críticas (GESTPIC):

  - WP.2 Requisitos de usuario
  - WP.3 Arquitectura del sistema
  - WP.4 Recogida de datos y correlación
  - WP.5 Visualización
  - WP.6 Integración y prototipado
  - WP.7 Evaluación y validación del sistema
- Proyecto *Scalable multidimensionAl sitUation awaReness sOlution for protectiNg european ports* (SAURON):
  - WP.3 User Requirements & Risk Scenarios
  - WP.4 Cyber Situation Awareness
  - WP.5 Physical Situation Awareness
  - WP.6 Hybrid Situation Awareness
  - WP.7 Communication with the Public & Interoperability
  - WP.8 System Demonstration & Validation

1.4.4. Desarrollo software

En los proyectos CIUSAT, como punto de partida de la herramienta HYBINT, y GESTPIC se ha llevado a cabo la completa implementación de sendas soluciones mediante el desarrollo e integración del conjunto de módulos que conforman sus correspondientes arquitecturas y el diseño de respectivas interfaces de usuario (*Human-Machine Interface* (HMI)).

En el proyecto SAURON, el desarrollo se está centrando en la adaptación a las necesidades específicas de infraestructuras portuarias de los sistemas GESTOP [27], solución de *Command & Control* (C2) para uso civil del grupo de Sistemas y Aplicaciones de Tiempo Real Distribuidos (SATRD), y GESTPIC para la respectiva visualización de SA física, ciber e híbrida en dicho contexto.

1.5. Organización de la memoria

La memoria de la presente tesis doctoral está compuesta de siete capítulos estructurados de la siguiente manera:

- En el capítulo 2, tras introducir la situación actual en el ciberespacio y el concepto de infraestructura crítica, se describe el estado del arte en CySA y se presentan algunos de los trabajos y propuestas más relevantes.

- En el capítulo 3, se plantea una arquitectura genérica de SA conjunta para la protección de cualquier tipo de infraestructura crítica en el entorno híbrido y se detallan los diferentes módulos que la conforman.
- En el capítulo 4, se presenta en detalle la arquitectura del sistema GESTPIC y sus componentes como caso de aplicación del modelo expuesto de SA híbrida a una herramienta de visualización de la situación en el entorno ciber-físico para la protección de infraestructuras críticas.
- En el capítulo 5, se evalúa exhaustivamente un prototipo final del sistema GESTPIC presentando, para ello, el escenario de pruebas empleado así como el conjunto de tests funcionales llevados a cabo.
- En el capítulo 6, se introduce el sistema HYBINT, una propuesta innovadora que aplicaría la arquitectura presentada de SA híbrida a una solución avanzada de inteligencia basada en la agregación y el análisis de información procedente de fuentes diversas.
- En el capítulo 7, se exponen las principales conclusiones derivadas de la presente tesis doctoral así como las líneas futuras de investigación más relevantes.
- Por último, se listan todas las referencias consultadas que han contribuido al desarrollo de la presente investigación.

Capítulo 2

Estado del arte

2.1. Introducción

Antes de nada, se hace necesaria la introducción de una serie de conceptos relacionados con la línea de investigación en la que se inscribe la presente tesis doctoral: el *Cyber Command & Control*, es decir, la aplicación de los sistemas de información para mando y control al ciberespacio.

Por tanto, ¿a qué hace referencia el concepto de C2? El *Department of Defense* (DoD) [28], a través del *Dictionary of Military and Associated Terms (JP 1-02)* [29], define el término de mando y control como:

"The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission."

La vista tradicional del mando y control viene representada por el concepto del bucle *Observe, Orient, Decide and Act* (OODA), introducido por J. Boyd con el fin de analizar el proceso de toma de decisiones en el transcurso de una operación (Figura 2.1) [30]. Se trata de un proceso cíclico en cuatro fases que se inicia con la observación (percepción) del dominio físico, continúa con el análisis (interpretación) de la información extraída que, junto al conocimiento previo del individuo, le sirve de orientación para decidir las acciones más oportunas a ejecutar y actuar en consecuencia. La aplicación de las acciones sobre el entorno modifica la situación del mismo, retroalimentando así el proceso de manera continuada.

También según [29], los sistemas de mando y control (C2S) quedan por tanto definidos como:

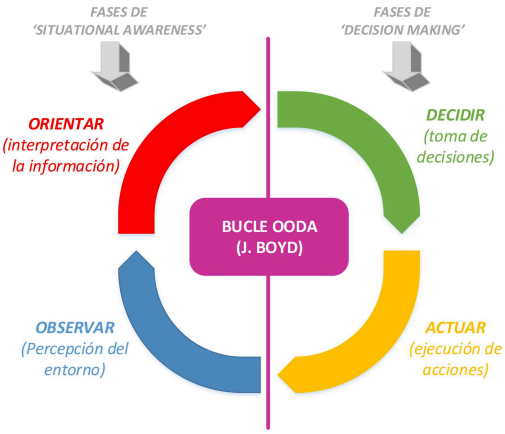


Figura 2.1: Vista tradicional de Mando y Control: bucle OODA.

"The facilities, equipment, communications, procedures, and personnel essential for a commander to plan, direct, and control operations of assigned and attached forces pursuant to the missions assigned."

Similar definición propone la Organización del Tratado del Atlántico Norte (OTAN) [31] en el *NATO Glossary of Terms and Definitions (AAP-06)* [32]:

"An assembly of equipment, methods and procedures and, if necessary, personnel, that enables commanders and their staffs to exercise command and control."

Para [33], los sistemas de mando y control deberán principalmente contribuir a los siguientes aspectos:

1. La obtención de información.
2. El procesado, análisis, síntesis, visualización y difusión, tanto vertical como horizontalmente, de dicha información.
3. El planeamiento y toma de decisiones.
4. La transmisión de órdenes a los mandos subordinados.
5. De nuevo, el control de la evolución de la situación según el ciclo OODA.

En [34], D. Alberts considera los sistemas *Command, Control, Communications, Computers, Intelligence, Surveillance & Reconnaissance* (C4ISR) como

una evolución natural de los sistemas C2, empujada por el avance tecnológico, que resalta el papel fundamental de las comunicaciones, la computación, la inteligencia, la vigilancia y el reconocimiento en las tareas del mando y control.

La fases de observación y orientación del ciclo OODA resultan claves en la correcta toma de decisiones pues es en ellas en las que el individuo adquiere realmente consciencia de la situación (o *Situational Awareness*). Pero, ¿qué implica exactamente el concepto de consciencia situacional? Pese a las diversas posturas existentes acerca de esta cuestión [35][36][37][38], la definición establecida por M. Endsley es sin duda la más extendida [39]:

"... is the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future."

En [40], M. Endsley defiende un modelo jerárquico de SA en tres niveles, trasladables a diferentes fases del bucle OODA, y que responde a una cadena de procesamiento de la información desde la percepción hasta la predicción pasando por la interpretación (Figura 2.2):

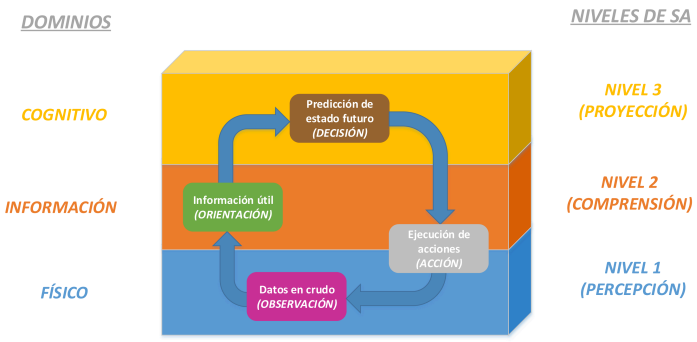


Figura 2.2: Modelo de *Situational Awareness* en tres niveles.

- **Nivel 1 de SA** (*Dominio físico – Observación*): percepción de los elementos en el entorno. Recepción inicial de información en su forma bruta y sin interpretación alguna de los datos en crudo.
- **Nivel 2 de SA** (*Dominio de la información – Orientación*): comprensión de la situación actual. Integración de los datos a los conocimientos previos extrayendo la información relevante para producir una *Common Opera-*

tional Picture (COP) del entorno, es decir, conocimiento actualizado del mismo.

- **Nivel 3 de SA** (*Dominio cognitivo – Decisión*): predicción del estado futuro. Capacidad de proyectar el futuro de los elementos del entorno y anticiparse a las situaciones venideras para planificar las acciones a ejecutar.

En otros trabajos de la autora en esta línea, se ha presentado un proceso de diseño de sistemas de información orientados a SA [41], se ha establecido un marco teórico para la representación de la SA de los niveles 2 y 3 en los sistemas de información basados en agentes [42] y se ha introducido *Situation Awareness Global Assessment Technique* (SAGAT) como técnica de evaluación de la consciencia situacional de un conjunto a través de la obtención de medidas objetivas de la SA de los individuo [43].

En este punto, es por tanto factible definir el término de *Cyber Situational Awareness* como la aplicación del concepto de consciencia situacional al ámbito del ciberespacio, donde este último viene definido por [29] como:

"A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."

En las siguientes secciones del presente capítulo se analizarán las principales amenazas, atacantes y vulnerabilidades que hoy en día existen en el ciberespacio; se definirán y clasificarán las infraestructuras críticas y sus interdependencias; y se presentarán los trabajos en el área de la CySA más relevantes que han sido estudiados haciendo especial hincapié en aquellos aspectos que son fundamentales en la presente tesis doctoral: las diferentes fuentes de datos ciber, los principales métodos de análisis de datos existentes y las técnicas de visualización de la información más relevantes.

2.2. Situación en el ciberespacio

Tomando como base los recientes informes del CCN-CERT [20][21][44] y con el fin de proporcionar una visión general y actualizada de la situación en el ciberespacio, en los siguientes puntos se dará respuesta a las siguientes cuestiones básicas: ¿cuáles son los principales tipos de ciberataques existentes y cómo se llevan a cabo?, ¿quiénes se esconden tras estas amenazas?, ¿a quiénes van dirigidos y qué consecuencias entrañan? y, por último, ¿por qué se producen?

2.2.1. Tipos de ciberataque

A continuación, se describen brevemente los principales tipos de ataque presentes hoy en día en el ciberespacio y los métodos empleados para llevarlos a término.

- **Código dañino**

  Se entiende por *malware* o código malicioso aquel software desarrollado con la finalidad de infiltrarse en determinados equipos o sistemas de información bien sea con la intención de interrumpir su funcionamiento, tomar el control del mismo o sencillamente sustraer información de este.

  Sin lugar a dudas, esta tipología representa uno de los principales vectores de ataque en el ciberespacio. En efecto, a nivel nacional, más de la mitad de los casi 21.000 ciberincidentes gestionados por el CCN-CERT en 2016 fueron de tipo *malware*. Dentro de esta categoría, donde el troyano (*backdoor*) sigue siendo la modalidad predominante respecto a otras como virus o gusanos, cabe destacar el caso particular del *ransomware* (Figura 2.3 [45]).

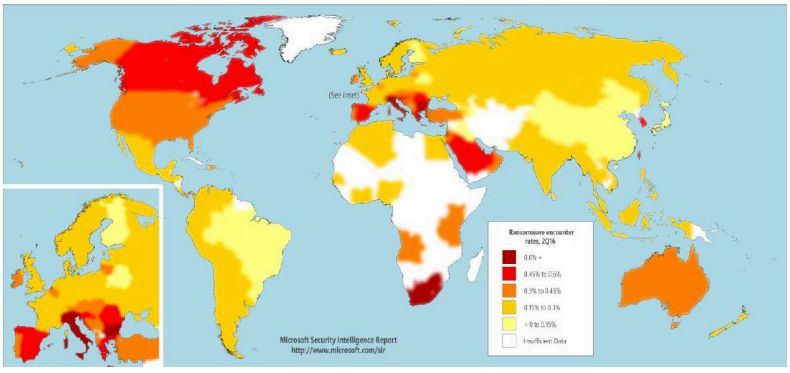


Figura 2.3: Tasa de incidencia de *ransomware* (abril-junio de 2016) [1].

El *ransomware* es una variante de código dañino enfocada al secuestro de equipos y sistemas, es decir, impide el acceso a la información de los mismos coaccionando al usuario a pagar un rescate por ellos. Es por tanto habitual su combinación con herramientas para el cifrado de la información (*cryptoware*). El número de infecciones por *ransomware* ha aumentado de manera exponencial a nivel mundial en los últimos años, sobretodo dirigido a los sectores de la energía, la sanidad, las telecomunicaciones o la

[1] Microsoft, "Microsoft Security Intelligence Report," *Microsoft Security*, vol. 21, 2016.

administración pública. Solo en España, el número de incidentes de este tipo gestionados por el CCN-CERT en 2016 ha crecido un 375 % respecto al año anterior. Sus implementaciones son cada vez más sofisticadas y sus ataques cada vez más dirigidos (y peligrosos) mediante el uso de depuradas técnicas de ingeniería social.

- **Publicidad dañina**

  Pese a que el *adware* es considerado por algunos como una variante más de *malware*, su objetivo inicial no es otro que el de exponer publicidad al usuario de manera, eso sí, intrusiva y muy molesta. Sin embargo, dicha publicidad se vuelve realmente dañina cuando, con la clara intención de atacar a los equipos de las víctimas, los mensajes comerciales introducidos en las páginas web han sido previamente infectados por los agentes o redes publicitarias que estas emplean. Tras ellos, suelen hallarse programas espía o *spyware* que, sin conocimiento ni consentimiento alguno del usuario, buscan la recolección de información del mismo y su distribución a terceros.

  Se trata de una amenaza de enorme magnitud por la ingente cantidad de visitas que reciben diariamente determinados sitios web muy populares donde son recurrentes ataques por *malvertising* altamente dirigidos a sectores concretos específicamente interesados en determinados productos [46]. Sin embargo, la solución no siempre pasa por la eliminación de la publicidad debido al considerable impacto negativo que supondría en un entorno donde el modelo de negocio está fundamentalmente basado en esta.

- **Suplantación de identidad**

  El *spoofing* consiste en suplantar la identidad de un determinado equipo en la red para acceder, de manera maliciosa, a los recursos de un tercer sistema basándose en algún tipo de confianza. Existen diversas técnicas de *spoofing* dependiendo del elemento de la comunicación falsificado: suplantación de dirección IP, DNS, web, etc.

  Las técnicas de suplantación representan el principal medio para acometer ataques de *phishing*, los cuales tienen por objetivo acceder a información confidencial de las víctimas (datos bancarios, contraseñas, credenciales de acceso, etc.) mediante prácticas de ingeniería social llevadas a cabo vía correo electrónico (*spam*), mensajería instantánea e incluso llamadas telefónicas.

  El *phishing* permanece como uno de los vectores de ataque más habituales debido a la dificultad para discernir entre un mensaje real y uno dañino;

lo cual, sumado a la cada vez más precisa determinación de sus víctimas, conlleva un elevado nivel de éxito [47].

- **Denegación de servicio**

  El ataque por denegación de servicio (*Denial of Service* (DoS)) es un ataque dirigido a una máquina o conjunto de máquinas con la finalidad de interrumpir temporal o definitivamente los servicios que ofrece. Su estrategia consiste en colapsar el equipo víctima mediante un número ingente de peticiones con el fin de consumir todos sus recursos (ancho de banda, ciclos de procesador, etc.) y no dejar espacio al procesamiento de peticiones legítimas.

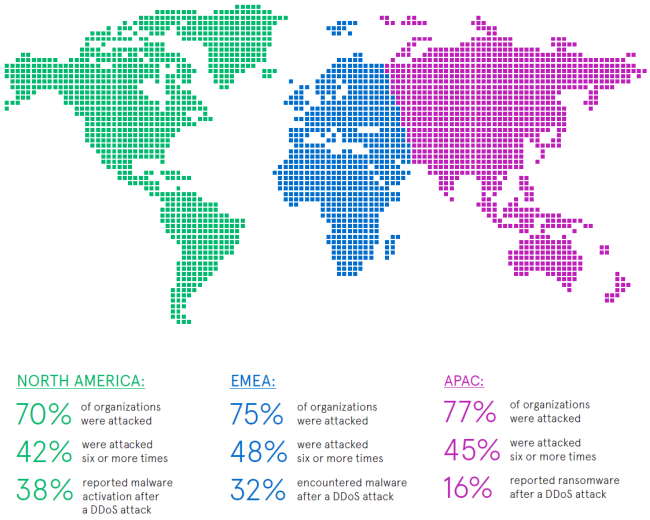


Figura 2.4: Incidencia de ataques DDoS (octubre de 2016) [2].

Se habla de DoS distribuida (DDoS) cuando, pretendiendo una todavía mayor incidencia del ataque, la DoS es ejecutada desde diferentes máquinas (normalmente, como se verá a continuación, *botnets*) distribuidas geográficamente.

La Figura 2.4, extraída de una encuesta mundial realizada en 2016 por Neustar [48] y que describe la incidencia de los ataques DDoS por continente [49], revela la magnitud que supone esta amenaza: en promedio, el 73 % de las organizaciones encuestadas sufrieron un ataque DDoS, el

[2] Neustar, Inc., "Worldwide DDoS Attacks & Protection Report," *Neustar Reports*, 2016.

45 % fueron atacadas seis o más veces y más del 25 % hallaron algún tipo de código dañino en sus sistemas tras los ataques.

Resulta además preocupante el reducido nivel de conocimientos necesario para perpetrar este tipo de ataques teniendo en cuenta la abundante oferta de servicios comercializados en el mercado negro y la *deep web* para acometerlos. Por si fuera poco, la actual tendencia no tiene visos de cambiar en un futuro cercano ya que los atacantes encuentran en el avance tecnológico dos grandes ventajas: el crecimiento del número de dispositivos conectados a Internet y del ancho de banda de las redes posibilita ataques cada vez más distribuidos y potentes.

- **Ataques a aplicaciones web**

  Las aplicaciones web representan otro de los principales objetivos de los agentes de la amenaza, cuyos ataques van más allá de la desfiguración o *page hijacking* (modificación malintencionada de sitios web).

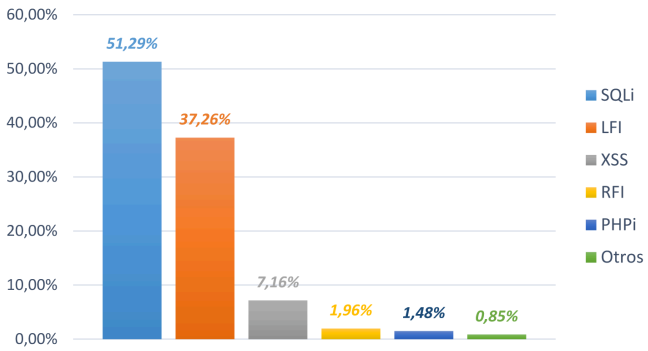


Figura 2.5: Ataques a aplicaciones web (octubre-diciembre de 2016) [3].

En efecto, tal y como refleja la Figura 2.5, el último informe de seguridad del año 2016 elaborado por Akamai [50] muestra la prevalencia de ataques por *SQL injection* (SQLi) y *Local File Inclusion* (LFI), los cuales constituyen la cuasi-totalidad de los mismos, frente a otros minoritarios como *Cross-Site Scripting* (XSS) [51].

[3] Akamai Technologies, Inc., "Q4 2016 State of the Internet / Security Report," *Akamai Research - The State of the Internet*, 2017.

- **Herramientas de ataque**

  La *deep web* representa el entorno habitualmente empleado por los atacantes para el intercambio de herramientas maliciosas y la planificación de ataques.

  Entendiéndose por *exploit* aquella aplicación que aprovecha (explota) una vulnerabilidad de un determinado sistema en beneficio propio, cabe indicar que la comercialización de herramientas automáticas de ataque (*exploits-kits*) representa una amenaza no despreciable que afecta tanto a equipos convencionales como dispositivos móviles o de comunicaciones.

  Además, las herramientas para la comisión de ataques DoS y las herramientas de acceso remoto (*Remote Access Tools* (RAT)) constituyen un recurso eficaz y económico para el desarrollo de todo tipo de actividades delictivas [52]. Estos sistemas van a menudo acompañados de soporte técnico por parte de sus creadores y son fácilmente localizables en foros clandestinos especializados en herramientas de *hacking* como *keyloggers*, herramientas de *spam* o *botnets* (máquinas zombi ejecutables de manera autónoma pero controladas por otra y habitualmente empleadas en ataques DDoS).

- **Servicios de buena fe**

  Con el fin de garantizar su anonimato en la red a la vez que se da alcance a un mayor número de potenciales víctimas, se ha probado la utilización por parte de los atacantes de determinados servicios muy populares como Dropbox [53], Google Docs [54] o Pinterest [55], para la dispersión inadvertida de *malware* aprovechando el cifrado por defecto del tráfico que atraviesa dichos servicios [56].

  La ubicuidad de los dispositivos móviles hoy en día en todo tipo de aplicaciones, personales o profesionales, sitúa también a estos, en particular a los de sistema operativo Android [57], como uno de los principales objetivos de los agentes de la amenaza. Nuevamente, el método de ataque pasa por la infección de sitios tradicionalmente confiables como son las tiendas oficiales de aplicaciones. Otro procedimiento igualmente empleado consiste en la infección de los propios entornos de desarrollo (*Integrated Development Environment* (IDE)), en ocasiones a través de atacantes infiltrados en los equipos oficiales de desarrollo.

2.2.2. Agentes de la amenaza

A continuación, se clasifican los agentes responsables de los incidentes y ataques en el ciberespacio así como sus principales motivaciones [58].

- **Estados**

  Las acciones dirigidas por los Estados, y en concreto por sus Servicios de Inteligencia, representan la mayor amenaza para la ciberseguridad nacional. Constituyen una alternativa real al espionaje tradicional debido a su bajo coste, a la gran cantidad de información obtenible y a la dificultad a la hora de demostrar su autoría.

  Las principales motivaciones de los Estados serían la obtención de información de la víctima relativa a seguridad y defensa nacional, propiedad intelectual o inteligencia sobre capacidades militares, el bloqueo de canales de comunicación del adversario en el ciberespacio y la realización de actividades subversivas en situaciones de crisis o conflicto.

- **Organizaciones criminales**

  El principal objetivo de las organizaciones criminales en el ciberespacio es la obtención de un beneficio económico directo (sustracción de credenciales) o indirecto (extorsión) de tanto a particulares como a organizaciones. El nivel de conocimiento de estos es muy variado abarcando desde especialistas (con alto nivel de profesionalidad e innovación) hasta grupos de bajo nivel.

  No deja de crecer la contratación del cibercrimen como un servicio mediante la utilización de la Internet profunda (*deep web*) para la planificación de ataques y el intercambio de herramientas. En ella, se ofertan servicios como la venta de código dañino (*malware*) listo para su uso, información sustraída de tarjetas bancarias, emails o redes sociales así como herramientas diseñadas para la comisión de acciones delictivas.

- **Organizaciones privadas**

  Pese a que las acciones emprendidas por las organizaciones privadas pueden ocasionalmente pretender la disrupción de los sistemas de información de los adversarios, la principal motivación de estas no deja de ser el denominado ciberespionaje industrial. Es decir, la ejecución de ataques para la obtención de información de la competencia bien sea para su uso en beneficio propio o para su venta a terceros.

- **Ciberterroristas**

  Los grupos terroristas en general, y los yihadistas en particular, hacen también uso del dominio ciberespacial para la realización de tareas que no impliquen directamente la ejecución de atentados, sino más bien labores de reclutamiento, adoctrinamiento o logística a través de páginas web propias o redes sociales.

- **Ciberactivistas (*Hacktivistas*)**

  Las acciones llevadas a cabo por estos grupos tienen justificación ideológica, están consideradas como una forma de activismo insurgente y su finalidad es visibilizar o reivindicar una causa concreta.

  La actividad de grupos ciberactivistas se centra en ataques de denegación de servicio (DoS) a objetivos gubernamentales, medios de comunicación u organizaciones privadas con el fin de desvelar determinados comportamientos o datos personales. Sus capacidades son variadas, pudiendo llegar a alcanzar altos niveles de sofisticación.

- **Cibervándalos y *script kiddies***

  Los cibervándalos desarrollan sus acciones como un reto personal, para demostrar sus propias capacidades o como una sencilla broma; por lo que las consecuencias no suelen ser habitualmente excesivamente graves. Aun así, la actividad de este tipo de grupos no ha dejado de crecer gracias a la proliferación de herramientas para la perpetración de ataques.

- **Actores internos (*Insiders*)**

  Se trata habitualmente de empleados o ex-empleados descontentos que, movidos por cuestiones personales, económicas o políticas, manipulan intencionadamente los sistemas de seguridad de su organización con el fin de sustraer información sensible, afectar los sistemas de almacenamiento o incluso causar graves disrupciones.

- **Ciberinvestigadores**

  Los ciberinvestigadores son en ocasiones responsables involuntarios de determinados ataques al exponer las vulnerabilidades descubiertas de los sistemas analizados cuando no se respeta la difusión responsable de las mismas, exhibiendo públicamente de este modo un nivel de seguridad inadecuado.

A modo de resumen, la Tabla 2.1 presenta los principales agentes de la amenaza y sus habituales motivaciones.

Actores	Motivaciones
Estados	Mejora de posición geopolítica o estratégica
Organizaciones criminales	Beneficio económico directo o indirecto
Organizaciones privadas	Obtención de información valiosa (ciberespionaje industrial)
Ciberterroristas	Atemorizar a la población, influir en decisiones políticas, propaganda o adoctrinamiento
Ciberactivistas	Ideológica (reivindicación de causas)
Cibervándalos	Evidenciar vulnerabilidades, retos, piratería o diversión
Actores internos	Venganza, beneficio económico o motivos ideológicos
Ciberinvestigadores	Evidenciar vulnerabilidades

Tabla 2.1: Atacantes y sus principales motivaciones.

2.2.3. Víctimas y consecuencias

Los ataques perpetrados en el ciberespacio dependen tanto del actor que los lleva a cabo como de las víctimas a quienes van dirigidos. A continuación, se describen los ciberincidentes mayoritariamente sufridos por cada tipo de objetivo: administración pública, organizaciones privadas y ciudadanía [58].

- **Administración pública**

  Las organizaciones del sector público son objetivo de la cuasi-totalidad de los ciberatacantes. Las acciones más significativas son el ciberespionaje político de los Estados o la disrupción de sistemas orquestada por organizaciones criminales, terroristas o cibervándalos. Le siguen acciones como el robo y publicación o venta de información por ciberactivistas, ciberinvestigadores, cibervándalos o actores internos. Por último, cabe también reseñar las tareas de propaganda o reclutamiento de ciberterroristas.

- **Organizaciones privadas**

  Las empresas y organizaciones del sector privado son fundamentalmente víctimas del ciberespionaje de naturaleza, en este caso, económica o industrial por parte de Estados u otras organizaciones privadas. Por otra

parte, destacan acciones de organizaciones criminales como el robo y publicación o venta de información, la toma de control de sistemas; así como actividades de propaganda y reclutamiento por parte de grupos terroristas, en particular, yihadistas. Aunque en menor medida, también son víctimas de la sustracción de información y disrupción de sistemas por parte de ciberactivistas y cibervándalos.

- **Ciudadanía**

  Los principales autores de los ataques contra ciudadanos (usuarios particulares) son las organizaciones criminales con fines como el robo y venta de información o la toma de control de sistemas; así como los grupos ciberyihadistas con intenciones propagandísticas y de reclutamiento.

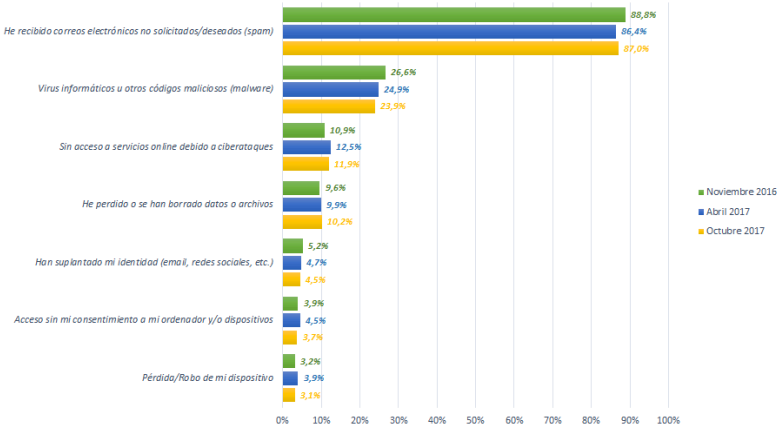


Figura 2.6: Incidentes sufridos por ciudadanos españoles [4].

En menor grado son también víctimas del ciberespionaje de los Estados o de la reventa de información corporativa por parte de organizaciones privadas.

La Figura 2.6, elaborada a partir de los recientes estudios sobre el estado de la ciberseguridad en los hogares españoles [59][60][61] del Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (ONTSI) [62], ilustra la tasa de ocurrencia de los incidentes más comúnmente sufridos por usuarios particulares a nivel nacional.

[4] Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (ONTSI), "Estudio sobre la Ciberseguridad y Confianza en los hogares españoles," ONTSI, Madrid, Spain, Tech. Rep. Nov. 2016, Apr. 2017, and Oct. 2017.

Como bien es sabido, una de las principales consecuencias de cualquier tipo de ciberincidente son los costes económicos derivados del daño, disrupción o destrucción provocados por este. En efecto, las consecuencias de los ciberataques pueden evaluarse mediante un coste global que deriva de varios costes parciales: costes económicos directos, costes de servicios, costes de imagen o de reputación, sanciones, etc.

Sin embargo, tal y como muestra la Tabla 2.2, los costes asociados a incidentes de seguridad y su gestión van más allá del factor económico.

Tiempo de inactividad	Pérdidas económicas y daños a la reputación. En el caso de empresas de gestión de servicios públicos, millones de personas se verían afectadas.
Costes económicos	Costes derivados de la respuesta a incidentes, de responsabilidad económica frente a clientes o de sanciones legales.
Pérdida de datos	Pérdida de registros de la empresa, de información personal de clientes o de propiedad intelectual puede afectar a las finanzas y a la reputación. Posible extorsión de ciberdelincuentes para obtener mayores beneficios económicos.
Pérdida de vidas	En el caso del sector sanitario, sistemas y equipamiento médico comprometidos ponen en riesgo la vida de pacientes por imposibilidad de acceso a registros e historias clínicas, prescripciones incorrectas o retraso en tratamientos.

Tabla 2.2: Principales costes derivados de ciberincidentes.

2.2.4. Principales vulnerabilidades

Los agentes de la amenaza viven de la explotación de vulnerabilidades para llevar a cabo sus ciberataques. La eliminación (o, cuanto menos, la minimización) de las mismas debe ser por tanto una prioridad para cualquier víctima potencial. Las vulnerabilidades existentes pueden resumirse tanto al software en sí como al factor humano.

- **El software**

  La industria del software se asemeja cada vez más a una cadena de montaje donde el producto final es resultado de la reutilización de componentes

ya existentes. La reutilización de elementos que presentan vulnerabilidades implica, por tanto, la fabricación de nuevos productos igualmente vulnerables [63].

Además, la inacción o dejadez de las organizaciones a la hora de llevar a cabo las actualizaciones de seguridad necesarias para solventar vulnerabilidades conocidas es motivo de muchas de las brechas de seguridad al permitir la aparición y uso de herramientas que las aprovechan. Esta situación resulta aún más crítica en el caso de los *Industrial Control Systems* (ICS) debido a, como se verá en la siguiente sección, los potenciales efectos cascada causados por las interrelaciones entre estos.

Cabe también resaltar el déficit de herramientas de seguridad, sobretodo en Pequeñas y Medianas Empresas (PyMEs) y organizaciones, donde el conjunto de medidas anti-amenaza existentes se limitan, en muchas ocasiones, al software antivirus únicamente (a menudo, además, desactualizado).

Por otra parte, la formación de los desarrolladores en materia de seguridad es todavía escasa y repercute en el software en sí, donde funcionalidad y velocidad priman frente a un comportamiento seguro del mismo.

Por último, la exhibición pública de las vulnerabilidades (habitualmente de naturaleza técnica) por parte de las organizaciones a través de estudios o informes publicados por la misma constituye, sin duda, otra fuente de vulnerabilidades a destacar [64].

- **El usuario**

  La compra de dispositivos móviles a nivel mundial mantiene un ritmo elevado [65]. La presión del mercado lleva a los fabricantes a comercializar nuevos productos cada año, limitando la vida útil de los mismos que, transcurrido ese tiempo, se convierten en potenciales víctimas de ciberataques al dejar de recibir soporte en forma de actualizaciones de seguridad.

  Pero no se trata únicamente de dispositivos móviles. En general, el número de dispositivos inteligentes (*smartwatches*, *smart TV*, electrodomésticos u otros *gadget*) conectados a Internet sigue creciendo sin cesar con la llegada del IoT. La multiplicidad de apartados y aplicaciones conectados a la red que estén siendo utilizados conteniendo graves vulnerabilidades supone un riesgo cada vez mayor para la seguridad.

  Además, en lo que a ingeniería social se refiere, los atacantes continúan día a día mejorando sus técnicas de engaño a víctimas para persuadirlas de cometer determinadas acciones. Que siga creciendo el número de

usuarios, tanto particulares como corporativos, víctimas de *phishing* vía correo electrónico o llamadas telefónicas denota una falta de sensibilización en materia de ciberseguridad. Así lo ilustra la Figura 2.7, extraída del barómetro en materia de ciberseguridad del año 2015 coordinado por la Dirección General de Comunicación de la Comisión Europea [66], donde queda reflejado cuan de informados se sienten los ciudadanos europeos acerca de los riesgos asociados a la ciberdelincuencia.

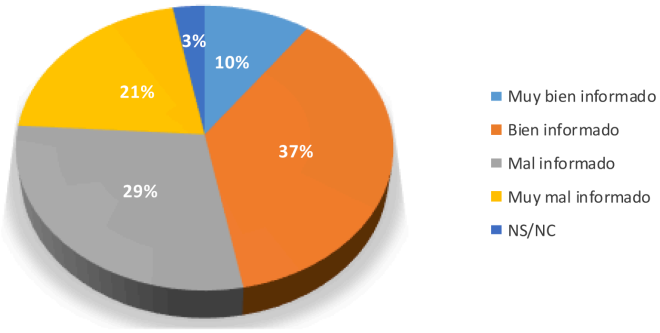


Figura 2.7: Grado de ciberconcienciación de ciudadanos europeos [5].

2.3. Infraestructuras críticas

2.3.1. Definición de infraestructura crítica

En diciembre de 2008, el Consejo de la Unión Europea publica la Directiva en Infraestructuras Críticas Europeas [67], donde se establece un procedimiento para la identificación y designación de las mismas. En el art. 2.a, estas quedan definidas como todos aquellos activos y sistemas de un estado cuyo mantenimiento resulta imprescindible para el buen funcionamiento del conjunto de la nación:

"... means an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of

[5] European Commission, "Special Eurobarometer 423: Cyber security," *European Union Open Data Portal*, Mar. 2015.

which would have a significant impact in a Member State as a result of the failure to maintain those functions."

A nivel nacional, es la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas [68] quien, en su art. 2.e, define estas últimas como:

"... infraestructuras estratégicas cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales."

Dado que el ataque o daño a una infraestructura crítica puede conllevar efectos desastrosos para la seguridad de un país y el bienestar de sus ciudadanos, minimizar las vulnerabilidades e incrementar la resiliencia de estas supone hoy en día uno de los principales objetivos de la Unión Europea [69]. Es por tanto necesario garantizar un nivel óptimo de protección y reducir en la medida de lo posible las consecuencias negativas derivadas de la disrupción o destrucción de cualquiera de estas infraestructuras. Pero, ¿qué significa realmente "protección" en este contexto? El art. 2.e de [67] define el concepto de protección de las infraestructuras críticas como:

"... means all activities aimed at ensuring the functionality, continuity and integrity of critical infrastructures in order to deter, mitigate and neutralise a threat, risk or vulnerability."

En España, la Ley 8/2011 [68] establece el concepto de protección aplicado a las infraestructuras críticas, en su art. 2.k, de la siguiente manera:

"... el conjunto de actividades destinadas a asegurar la funcionalidad, continuidad e integridad de las infraestructuras críticas con el fin de prevenir, paliar y neutralizar el daño causado por un ataque deliberado contra dichas infraestructuras y a garantizar la integración de estas actuaciones con las demás que procedan de otros sujetos responsables dentro del ámbito de su respectiva competencia."

2.3.2. Clasificación de infraestructuras críticas

A tal fin, el *European Programme for Critical Infrastructure Protection* (EPCIP) [70] es el responsable de establecer un marco genérico de actividades enfocadas a mejorar la protección de las infraestructuras críticas en Europa frente a amenazas de tipo terrorista, actividades criminales, desastres naturales o accidentes de otro tipo. A nivel nacional, el Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC) [71] es el órgano ministerial

dependiente de la Secretaría de Estado de Seguridad [72] responsable de supervisar, a través del Plan Nacional de Protección de las Infraestructuras Críticas (PNPIC), las actividades relacionadas con la protección de las infraestructuras críticas (art. 7 de la Ley 8/2011 [68][73]).

La Tabla 2.3 presenta, de manera resumida, las categorías (o sectores) de infraestructuras críticas establecidas por el EPCIP y su correspondiente descripción [74].

Sector	**Descripción**
Energía	Fuentes de producción, concentradores y distribuidores de energía (electricidad, gas y petróleo)
TIC	Sistemas de info. e Internet, comunicaciones fijas y móviles, comunicaciones radio y navegación, comunicaciones satélite y *broadcasting*
Agua	Suministro de agua (p. ej. presas), control de cantidad y calidad del agua
Agricultura y Alimentación	Suministro, salubridad y seguridad alimenticia
Medicina y Salud Pública	Cuidados médicos y hospitalarios, medicamentos, vacunas y farmacología, laboratorios y agentes biológicos
Sistemas Financieros	Banca, servicios de pago y asignaciones financieras gubernamentales
Administración Pública	Instalaciones gubernamentales, fuerzas armadas, administración civil, servicios de emergencia, servicio postal
Seguridad y Orden Público	Mantenimiento del orden público y legal, seguridad y protección, administración legal y judicial
Transportes	Transporte terrestre, ferroviario y tráfico aéreo, vigilancia fronteriza, vías fluviales y transporte marítimo
Industria Química	Producción, almacenaje y transporte de sustancias y bienes peligrosos
Industria Nuclear	Producción y almacenaje de material nuclear

Espacio	Comunicaciones e investigación
Investigación	Instalaciones de investigaciones mayores

Tabla 2.3: Clasificación de infraestructuras críticas.

Adicionalmente a los anteriores, el DHS de los Estados Unidos, a través de su *National Infrastructure Protection Plan* (NIPP), define también como sectores críticos los descritos en la Tabla 2.4.

Sector	**Descripción**
Monumentos e Iconos Nacionales	Monumentos, objetos o lugares de representación de la cultura nacional o de importancia política o religiosa
Instalaciones Comerciales	Centros comerciales, inmuebles de oficinas, recintos deportivos y demás espacios de gran aforo
Producción Crítica	Transformación de materiales en bienes, incluyendo todos los procesos de fabricación y transporte
Industria de Defensa	Instalaciones de producción de recursos militares (p. ej. armamento, flota aérea y naval) y mantenimiento de los servicios esenciales para la seguridad nacional

Tabla 2.4: Sectores críticos adicionales.

2.3.3. Interdependencia de infraestructuras críticas

La Figura 2.8, extraída de un informe de la *European Union Agency for Network and Information Security* (ENISA) [75] de 2016 donde se revisan los estudios existentes sobre el impacto económico de ciberincidentes en infraestructuras críticas [76], refleja la gran variedad de ataques reportados por cada uno de los sectores críticos.

Además y en la mayoría de los casos, dichas infraestructuras críticas, lejos de ejercer sus funciones de manera aislada, están conectadas entre sí a través

de relaciones de interdependencia que van más allá del sector al que pertenecen: una infraestructura crítica podría depender de los productos y servicios provistos por una segunda al igual que esta podría requerir de los productos y servicios facilitados por la primera.

		Number of studies per sector									
Nr.	Attack / Threat	Public Administration	Energy	Health	Financial	ICTs	Transport	Water	Aerospace	Food	Chemistry
1	Malware	7	10	7	9	9	7	1	1	1	1
2	DoS/DDoS	10	8	8	11	11	8	1	1	1	–
3	Cyber Espionage	2	3	3	3	2	1	1	1	–	1
4	Web-Based Attacks	5	7	4	7	7	6	–	1	1	–
5	Insider Threat	7	4	6	8	7	3	–	1	1	–
6	Hacktivism	3	3	3	5	4	–	–	1	1	1
7	Malicious Code	5	6	5	7	7	6	–	–	–	–
8	Phishing	6	4	4	6	6	4	1	–	–	–
9	Web Application Attacks	5	2	4	4	4	2	1	–	–	–
10	Ransomware	3	1	3	2	2	1	1	–	–	–
11	Botnets	1	2	2	2	2	2	–	–	–	–
12	Critical Vulnerabilities	1	1	1	–	–	1	1	–	–	–

Figura 2.8: Tipos de ataque por sectores críticos [6].

Bajo este contexto, la disrupción, daño o destrucción de una infraestructura crítica puede provocar un efecto cascada sobre múltiples infraestructuras vinculadas a esta.

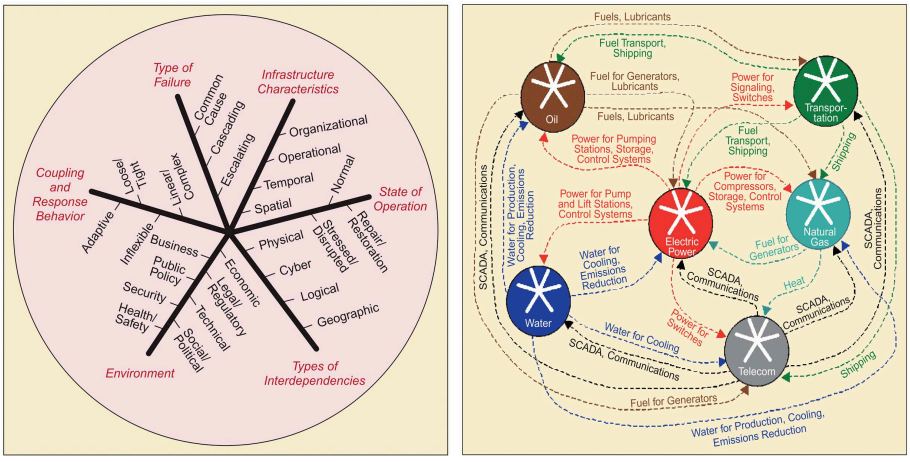
En [77] se identifican y analizan las interrelaciones entre las diferentes áreas de control de los sistemas ciber-físicos industriales (sistemas *Supervisory Control And Data Acquisition* (SCADA) [78]).

En [79] se establece una taxonomía de las interdependencias entre infraestructuras críticas basada en seis dimensiones (Figura 2.9(a)): tipo de interdependencia, sector de la infraestructura, tipo de emparejamiento y respuesta, tipo de fallo, tipo de infraestructura y estado de la operación. La Figura 2.9(b) muestra un ejemplo de interdependencias entre infraestructuras críticas de diferentes sectores. Respecto al tipo de interdependencia en particular, los autores distinguen entre los siguientes cuatro:

- **Física:** cuando una infraestructura crítica requiere de los recursos o materiales de otras infraestructuras.

[6] ENISA, "The cost of incidents affecting CIIs," *ENISA Publications*, Aug. 2016.

- **Geográfica:** cuando múltiples infraestructuras pueden verse afectadas por un incidente acontecido en una de ellas debido a la proximidad entre todas estas.
- **Ciber:** cuando existe una dependencia de los sistemas de información y comunicaciones.
- **Lógica:** cuando los sistemas, acciones o decisiones que conectan a agentes de diferentes infraestructuras no tienen naturaleza física, geográfica ni ciber (p. ej. decisiones políticas o burocráticas).



(a) (b)

Figura 2.9: Interdependencia de infraestructuras críticas (Rinaldi *et al.*) [7].

Proyectos europeos como *Multi-ordEr Dependency approaches for managing cascading effects in ports' global sUpply chain and their integration in riSk Assessment frameworks* (MEDUSA) [80] del *Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme* (CIPS) [81], o *Multidimensional, IntegraTed, rIsk assessment framework and dynamic, collaborative Risk ManaGement tools for critical information infrAstrucTurEs* (MITIGATE) [82][83] y SAURON [84] del *Horizon 2020 Programme* (H2020) [85] hacen especial hincapié en los efectos cascada causados por daños o ataques a infraestructuras críticas [86].

[7] S. M. Rinaldi *et al.*, "Identifying, understanding, and analyzing critical infrastructure interdependencies," *IEEE Control Systems*, vol. 21, no. 6, pp. 11-25, Dec. 2001.

Finalmente, en [87] se propone una serie de medidas a llevar a cabo para garantizar la protección de las infraestructuras críticas:

1. Evaluar las vulnerabilidades de las infraestructuras críticas frente a potenciales ataques físicos y ciber.

2. Desarrollar planes para la eliminación de las vulnerabilidades más significativas.

3. Proponer sistemas para la identificación y prevención frente a intentos de ataques mayores.

4. Implementar planes para alertar, contener y repeler ataques en curso.

5. Reconstituir rápidamente las funcionalidades mínimas esenciales en los instantes posteriores a un ataque.

2.4. *Cyber Situational Awareness*

2.4.1. Marco general

Los autores de [88], tras revisar más de un centenar de artículos de cuatro reconocidas bases de datos científicas, catalogan la literatura existente en lo que a CySA se refiere en las siguientes áreas principales de investigación: (i) conceptos generales de CySA, (ii) aplicación de CySA a los sistemas de control industrial (ICS), (iii) aplicación de CySA a la gestión de emergencias, (iv) aplicación de CySA al ámbito militar, (v) algoritmos, arquitecturas y sistemas, (vi) fusión de información de fuentes diversas, (vii) técnicas de visualización de CySA, (viii) especificaciones de diseño e interfaces HMI e (ix) interoperabilidad e intercambio de información CySA.

La principal conclusión que deriva de tan exhaustivo estudio es la abundancia de publicaciones en determinadas áreas como la CySA en los ICS, algoritmos o técnicas de fusión de información en los sistemas de detección de intrusiones frente a la carencia de trabajos en ámbitos como la compartición de información para CySA o la evaluación de daños durante operaciones militares. Pese a ello, trasciende un notorio interés por incrementar la investigación empírica en ciertos campos todavía por explorar.

Enfoques teóricos

Ya en el proyecto europeo PANOPTESEC [89] del *7th Framework Programme* (FP7) [90], orientado a la seguridad de la información, se ahonda en la producción y visualización de una CySA de redes de sistemas aunque sin considerar, eso sí, la idea de una COP conjunta del entorno ciber-físico.

En [91] se argumenta en profundidad la necesidad de conducir operaciones conjuntas en los escenarios de tierra, mar, aire, espacio y ciberespacio.

Por su parte, en [92], se apuesta por investigar soluciones para la obtención de CySA en los niveles superiores del modelo de SA de M. Endsley desarrollando algoritmos que mejoren el aprendizaje automático de los sistemas para automatizar los procesos cognitivos de toma de decisiones.

Los autores de [93] señalan las ventajas que ofrece combinar información HUMINT con herramientas de seguridad, a través de técnicas de fusión y filtrado de información, para mejorar la toma de decisiones en entornos dinámicos y complejos.

A su vez, en [94] se presenta un marco teórico general para la elaboración de una SA a gran escala para la protección de infraestructuras críticas a distancia.

Por último, en [95] se propone un modelo genérico cíclico de CySA en cinco fases (Figura 2.10): (i) análisis de la situación ciber, (ii) establecimiento de políticas de seguridad, (iii) monitorización del ciberespacio, (iv) respuesta frente a potenciales ataques y (v) conocimiento de las amenazas del entorno.

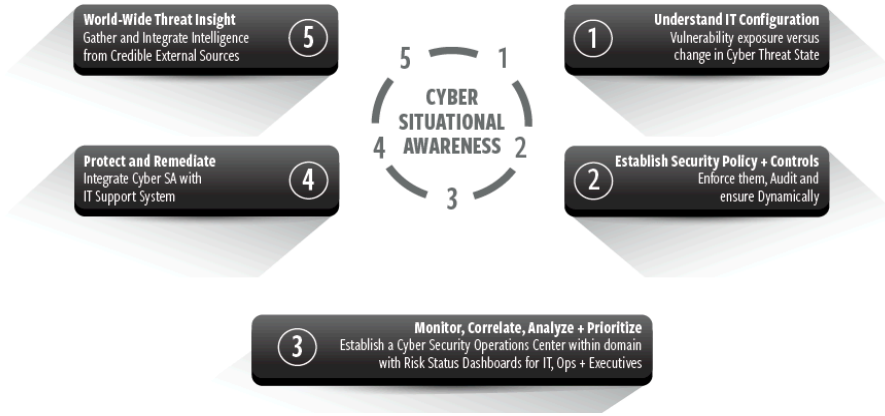


Figura 2.10: Modelo genérico de CySA en cinco fases (Matthews *et al.*) [8].

[8] E. D. Matthews *et al.*, "Cyber Situational Awareness," *The Cyber Defense Review*, vol. 1, no. 1, pp. 35-45, Spring 2016.

Métricas y estándares

En [96] se demuestra que las técnicas tradicionales de evaluación de SA, tales como SAGAT [43] o *Situational Awareness Rating Technique* (SART) [97], resultan inadecuadas en entornos *Command, Control, Communications, Computers & Intelligence* (C4I) por su ineficiencia al valorar la SA compartida en diferentes localizaciones de manera simultánea y en tiempo real.

Por su parte, los autores de [98] proponen unas métricas para la evaluación de los sistemas de SA en el dominio ciber basadas en cuatro dimensiones:

- **Confianza**: capacidad del sistema para detectar los indicios de un ataque real.
- **Pureza**: calidad de los indicios de ataque correctamente detectados.
- **Coste**: media ponderada de los ataques detectados en función de su tipo y riesgo.
- **Rapidez**: capacidad de respuesta del sistema en el tiempo requerido.

Por otro lado, en [99] se analizan las siguientes taxonomías, sistemas de puntuación y estándares de compartición de información, en su mayoría desarrolladas por la compañía Mitre [100] o por el *National Institute of Standards and Technology* (NIST) [101], y la aplicación de estas mismas a los ámbitos de la ciberseguridad y la ciberinteligencia:

- **Taxonomías**: TAL [102] de Intel [103]; NVD [104] del NIST; CVE [105], CPE [106], CWE [107], CAPEC [108] y ATT&CK [109] de Mitre.
- **Sistemas de puntuación**: CVSS [110] del NIST; CWSS [111] de Mitre.
- **Estándares de compartición**: STIX [112][113] y MAEC [114] de Mitre; OpenIOC de Mandiant [115].

De manera adicional, cabe también destacar otros proyectos de interoperabilidad como *Open Threat Exchange* (OTX) de AlienVault [116], *Security Content Automation Protocol* (SCAP) del NIST [117] o *Trusted Automated eXchange of Indicator Information* (TAXII) de Mitre [118].

Se constata, sin embargo, que ninguna ontología existente está realmente capacitada a día de hoy para ofrecer una inteligencia eficiente en el ciberespacio debido a la escasa madurez de sus desarrollos y a la falta de completitud de la información abarcada.

Capacidades y características de diseño

Los autores de [119] comparan dos aproximaciones diferentes en el diseño del HMI de sistemas para CySA: *user centered* (más apropiado para los procesos de análisis y visualización de datos dinámicos) y *system based* (preferible para una mejor comprensión del sistema y de sus limitaciones físicas y lógicas).

En [120] se estudia el carácter distribuido de la CySA y se propone el uso de herramientas y tecnologías que permitan un mayor intercambio de información entre los diferentes dominios para potenciar la CySA del conjunto mejorando la CySA individual de cada analista en su respectivo dominio funcional.

De igual manera, en [121] se apuesta por el uso de herramientas para el modelado y análisis de arquitecturas de sistemas ciber-físicos (*Cyber Physical Systems* (CPS)) con el fin de optimizar el diseño de los mismos en lo que medidas de rendimiento se refiere.

Por último, en [42] se enumeran las principales capacidades que debería de proveer, de manera general, un sistema de *Cyber Common Operating Picture* (CCOP) en el ámbito militar:

- Estado y localización física (y, cuando aplique, virtual), precisa y en tiempo real de los activos ciber propios, neutros y del enemigo.
- Capacidad de proporcionar C2 a las unidades amigas asignadas durante operaciones en el ciberespacio.
- Procesado y visualización continuos de la información de las dimensiones de tierra, mar, aire, espacio y ciberespacio.
- Adecuada SA del entorno en los niveles táctico, operacional y estratégico.
- Análisis predictivo para anticipar y reaccionar a las acciones del enemigo.
- Soporte a la toma de decisiones en operaciones sobre el espacio ciberfísico.

Algunos modelos y propuestas

En [122], los autores sugieren una serie de recomendaciones para la investigación y desarrollo de los CPS en general y que pueden resumirse a: (i) arquitecturas y abstracciones estandarizadas para un diseño modular de los CPS, (ii) nuevos algoritmos y herramientas para la fiabilidad y seguridad de los CPS en entornos complejos y (iii) componentes hardware y software altamente confiables y reconfigurables para los futuros CPS.

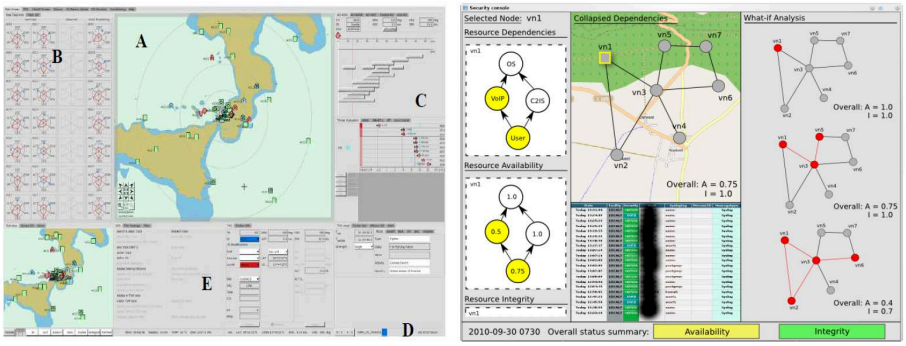
Por otro lado, [123] analiza y compara diferentes tecnologías de Internet (Google Web Toolkit [124], jQuery [125], Adobe Flex [126] y Microsoft Silverlight [127]) para el desarrollo de aplicaciones cliente en sistemas de protección de infraestructuras críticas.

En [128], se presenta una arquitectura para una mejor evaluación de la CySA consistente en un avanzado mecanismo de razonamiento de la información relevante con el fin de ofrecer una mejora en la toma de decisiones a los analistas de inteligencia.

Los autores de [129] evalúan la eficiencia de los CPS frente a ataques maliciosos en el contexto de la gestión de emergencias.

Una infraestructura ciber es propuesta en [130] para validar un sistema de fusión de la información basado en HUMINT.

Finalmente, en [131] se abordan las tradicionales técnicas de visualización mediante interfaces en sistemas de ciberseguridad, constatando su ineficacia para la obtención de una adecuada CySA. Para ello, se proponen algunos avances en la visualización encaminados a integrar, sobre un interfaz tradicional, información georreferenciada de cibereventos (Figura 2.11(a)) mediante el uso de representaciones basadas en grafos con nodos y enlaces (Figura 2.11(b)).



(a) (b)

Figura 2.11: Interfaz de visualización de CySA (Klein *et al.*) [9].

En la Tabla 2.5 se listan las capacidades, tanto de visualización como de interacción, que los autores proponen para cada uno de los sectores de la interfaz de visualización.

[9] G. Klein *et al.*, "Towards a Model-Based Cyber Defense Situational Awareness Visualization Environment," in *Proceedings of the RTO workshop "Visualising Networks: Coping with Chance and Uncertainty" (RTO-MP-IST-093)*, Rome, New York, United States, Oct. 19-21, 2010, pp. 1-11.

Sector	Capacidades de visualización e interacción
A	*Visualización* • Mapa de recursos ciber o georreferenciados *Interacción* • Modificación de nivel de abstracción mediante zoom • Herramienta de selección de múltiples recursos
B	*Visualización* • Recursos internos de nodos seleccionados en A y sus relaciones • Análisis de dependencias entre recursos *Interacción* • Herramienta de selección para análisis de dependencias
C	*Visualización* • Visualización de múltiples reconfiguraciones posibles/opciones de respuesta al ataque en paralelo • Análisis de causa origen *Interacción* • Modo de edición para rápida modificación de indicadores de estado de recursos y sus dependencias
D	*Visualización* • Datos de estado global del sistema y estado de alerta global *Interacción* • Herramienta de selección de grupo de usuarios
E	*Visualización* • Indicadores de estado de recursos seleccionados en A • Panel de visualización de detalles de recursos críticos *Interacción* • Modo realce: resaltar autores de mensajes en A

Tabla 2.5: Capacidades de visualización e interacción (Klein *et al.*) [10].

De manera adicional, en [132] pueden consultarse algunas de las soluciones en el ámbito de la ciberseguridad desarrolladas, y algunas de ellas comercializadas, por la *Defense Information Systems Agency* (DISA) del DoD de los Estados Unidos.

[10] G. Klein *et al.*, "Towards a Model-Based Cyber Defense Situational Awareness Visualization Environment," in *Proceedings of the RTO workshop "Visualising Networks: Coping with Chance and Uncertainty" (RTO-MP-IST-093)*, Rome, New York, United States, Oct. 19-21, 2010, pp. 1-11.

2.4.2. Sensores y fuentes de datos

Tradicionalmente, la protección de los sistemas de información en la red se ha llevado a cabo de manera más bien preventiva o no intrusiva mediante diversos componentes de seguridad como *firewalls*, antivirus, escáneres o *Intrusion Detection System* (IDS)/*Intrusion Prevention System* (IPS). Estas técnicas, junto a otras como la ingeniería social o la inteligencia de fuentes abiertas (*Open Source Intelligence* (OSINT) [29]) permiten llevar a cabo la fase de reconocimiento pasivo (o exploración) de la *Cyber Kill Chain* [133][134], un modelo de defensa de sistemas de información frente a los ataques más avanzados en el ciberespacio (Figura 2.12). Por su parte, el reconocimiento activo (o rastreo) se basa en métodos más intrusivos como el escaneo de puertos y vulnerabilidades o la obtención y análisis de trazas.

Figura 2.12: *Cyber Kill Chain* [11].

Sin embargo, estas herramientas de defensa convencionales resultan por sí solas insuficientes ante las nuevas y sofisticadas ciberamenazas (*Advanced Persistent Threat* (APT) [135]), que buscan la ex-filtración constante de información de objetivos mediante la continua penetración en sus sistemas. En un contexto como el actual, donde los ataques son cada vez más complejos y distribuidos, se hacen necesarios componentes de seguridad en red más avanzados que ofrezcan capacidades de respuesta tanto preventivas, como proactivas y reactivas. En esta línea, adquieren especial relevancia los sistemas *Unified Threat Management* (UTM) y, en especial, los *Security Information and Event Management* (SIEM).

Los sistemas UTM son dispositivos que integran diversos componentes básicos de seguridad (antivirus, *firewalls*, IDS/IPS, *antispam*, *antispyware*, filtrado

[11] E. M. Hutchins *et al.*, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," in *Proceedings of the 6th International Conference on Information Warfare and Security 2011 (ICIW)*, Washington D.C., United States, Mar. 17-18, 2011, pp. 1-12.

de contenidos, etc.) en uno único [136]; lo que simplifica notablemente las tareas de gestión y mantenimiento a cambio, eso sí, de un riesgo mayor debido a la presencia de un único punto de fallo posible.

Por el contrario, los sistemas SIEM [137] no vienen a sustituir estos componentes de seguridad sino que se alimentan de la información que estos, desplegados en la red a modo de agentes o sensores, les proporcionan. A grosso modo, los SIEM recopilan, almacenan y correlan datos y *logs* (registros de eventos y acciones) de los equipos (hardware) y sistemas (software) en su red para detectar anomalías o actividades sospechosas y prevenir posibles ataques [138] (Figura 2.13); de ahí que su acrónimo resulte de la combinación de sus dos principales funcionalidades [139]:

- ***Security Information Management* (SIM)**: análisis de *logs*, reportes de seguridad y almacenamiento a largo plazo.
- ***Security Event Management* (SEM)**: monitorización en tiempo real, gestión de incidentes y notificaciones.

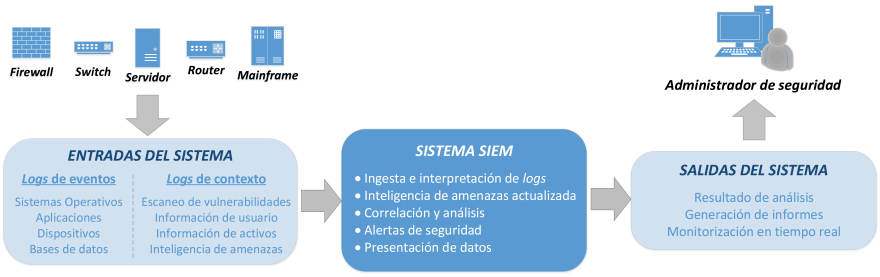


Figura 2.13: Funcionamiento genérico de un SIEM [12].

Las capacidades básicas que por tanto ofrece un sistema SIEM son las siguientes [140]:

- Colección de *logs* de múltiples agentes, normalización y filtrado de datos.
- Agregado de información de fuentes de inteligencia.
- Correlación de eventos y monitorización en tiempo real.
- Escaneo de vulnerabilidades y análisis forense.

[12] P. Rubens. (2017, Jun. 5) SIEM Guide: A Comprehensive View of Security Information and Event Management Tools, `https://www.esecurityplanet.com/network-security/security-information-event-management-siem.html` [Accessed Jul. 5, 2018].

- Almacenamiento de información a largo plazo.
- Generación de alertas de seguridad.
- Presentación de datos y generación de informes.

A continuación, se presentan algunas de las soluciones comerciales SIEM más destacadas en la actualidad [141][142][143][144].

- **AlienVault USM**

  AlienVault *Unified Security Management* (USM) [145] se presenta como una solución SIEM de bajo coste gracias a su propio protocolo de libre uso, OTX [116]. Incluye un servicio de suscripción que actualiza reglas de correlación, modelos de respuesta o firmas para comprobación de vulnerabilidades e intrusiones. Su versión gratuita *Open Source Security Information Management* (OSSIM) [146] es, hoy por hoy, la alternativa SIEM por excelencia gracias a su enorme aplicabilidad y excelente reputación. Puede llegar a gestionar 15.000 eventos por segundo y está disponible como dispositivo físico, máquina virtual o servicio en la nube.

- **Micro Focus ArcSight**

  La plataforma *ArcSight* de Micro Focus y Hewlett-Packard consiste en una solución SIEM de ámbito empresarial compuesta de las herramientas *ArcSight Express* [147] (orientada a despliegues de tamaño medio) y *ArcSight Enterprise Security Manager* (ESM) [148] (enfocada a implementaciones a mayor escala). El sistema es capaz de recolectar datos de más de 300 fuentes diferentes y analizar 75.000 eventos por segundo. La solución puede desplegarse como software, distribución virtual o servicio en la nube.

- **IBM QRadar**

  IBM *QRadar* [149] constituye el núcleo central de la plataforma IBM *QRadar Security Intelligence Platform*, la cual incluye también componentes adicionales que ofrecen funcionalidades extra como la gestión de *logs*, la monitorización de red, la gestión de vulnerabilidades o la evaluación de riesgos. Cuenta, además, con más de 400 módulos de soporte para la colección de datos y es capaz de evaluar miles de millones de eventos por día. Se distribuye como solución software, máquina virtual o servicio en la nube.

- **LogRhythm SIEM**

  La solución SIEM de LogRhythm [150] se conforma de un conjunto de componentes que pueden ejecutarse desde un dispositivo único o por separado como herramientas independientes: colector de datos, procesador e indexador de datos, motor de inteligencia artificial, gestor de la plataforma y servicios WebUI. La oferta de este SIEM también incluye reconocimiento de patrones, respuesta a incidentes y estimación de tendencias a largo plazo. El sistema está orientado a PyMEs y está disponible como software y como aplicación virtualizada.

- **Splunk ES**

  La plataforma de seguridad de Splunk se compone de Splunk *Enterprise* [151] como producto principal y de dos herramientas *premium*: *Enterprise Security* (ES) [152] y *User Behavior Analytics* (UBA) [153]. El software incluye un kit de herramientas de *machine learning* que permite al usuario efectuar análisis específicos y configurar sus propias correlaciones. En la actualidad, sus clientes procesan petabytes de datos al día. La solución se distribuye igualmente como software así como servicio en la nube.

- **McAfee ESM**

  McAfee ESM [154] es un sistema SIEM al uso que, más allá de las funcionalidades básicas, ofrece adicionalmente módulos específicos para la monitorización de la base de datos, la decodificación e inspección de tráfico y una fuente de inteligencia de amenazas producida por McAfee Labs. La plataforma procesa decenas de miles de eventos por segundo y puede almacenar miles de millones de eventos. Especialmente presente en los sectores público, educativo y sanitario, es adquirible como aplicación física o virtual.

- **RSA NetWitness**

  La *suite* RSA *NetWitness Platform* [155] está compuesta por los sistemas RSA *NetWitness Logs and Packets*, RSA *NetWitness Endpoint* y RSA *NetWitness Security Operations (SecOps) Manager*. La plataforma garantiza la escalabilidad mediante el despliegue de componentes adicionales como decodificadores, concentradores y archivadores. Esta solución, especialmente extendida en los sectores financieros, energéticos y de las TIC, puede procesar hasta 30.000 eventos por segundo y recolectar 10 gigabytes de datos por segundo.

Más allá de sistemas SIEMs, cabe también destacar otras soluciones interesantes como *Malware Information Sharing Platform and Threat Sharing* (MISP) [156] para el intercambio de información de eventos y amenazas ciber, *Request Tracker for Incident Response* (RTIR) [157] como extensión de la plataforma de *ticketing Request Tracker* (RT) [158] para la gestión y seguimiento de ciberincidentes, herramientas para análisis de paquetes (*sniffers*) como Wireshark [159] o Ettercap [160], para la búsqueda de vulnerabilidades como OpenVAS [161] o Nexpose [162], para la detección de intrusiones como Snort [163] o Suricata [164] y distribuciones como Metasploit [165] o Kali Linux [166] para la ejecución de test de penetración.

Por último, a nivel nacional cabe reseñar herramientas propias como Listado Unificado de Coordinación de Incidentes y Amenazas (LUCIA) [167], Centro de Análisis de Registros y Minería de Eventos (CARMEN) [168], Gestión de Logs para Respuesta a Incidentes y Amenazas (GLORIA) [169] o Procedimiento Informático-Lógico para el Análisis de Riesgos (PILAR) [170] del CCN-CERT [18] o la *suite* Emas de la compañía S2 Grupo [171].

2.4.3. Métodos y herramientas de análisis

Minería de datos y aprendizaje automático

En la actualidad, las principales técnicas de análisis de datos están fundamentalmente relacionadas con métodos analíticos orientados a *Big Data*, en particular, con dos conceptos íntimamente ligados entre sí: la minería de datos (*data mining*) [172] y el aprendizaje automático (*machine learning*) [173]. En efecto, se suele considerar la extracción de características inherentes a los datos y la predicción de su evolución como sub-procesos de uno único que, a partir de un conjunto de datos de entrada no estructurados, pronostica tendencias futuras.

En [174], el autor define el concepto de *data mining* como:

"... a process that uses a variety of data analysis tools to discover patterns and relationships in data that may be used to make valid predictions."

Por su parte, en [175] se entiende por *data mining* la siguiente definición:

"... is the iterative and interactive process of discovering valid, novel, useful, and understandable knowledge (patterns, models, rules etc.) in Massive databases."

En cuanto al concepto de *machine learning*, se encuentra bastante aceptada la definición dada por el autor de [176]:

"A computer program is said to learn from experience E with respect to some class of tasks T and performance measure P, if its performance at tasks in T, as measured by P, improves with experience E."

La minería de datos y el aprendizaje automático son campos que se superponen de manera significativa y que a menudo emplean mismas técnicas; por lo que es habitual que sus términos lleven a confusión o se empleen erróneamente. Sin embargo, pueden resumirse las ideas subyacentes a cada uno de estos conceptos de la siguiente manera:

- **Aprendizaje automático**: técnica que busca estudiar y elaborar un modelo o sistema capaz de aprender de los datos. Está centrada en la predicción de estados futuros a través del conocimiento adquirido a partir del entrenamiento de datos. Se aplica habitualmente en bases de datos de tamaño limitado para aumentar su precisión.
- **Minería de datos**: proceso de extraer información de un conjunto de datos y estructurarla de manera comprensible para su uso. Trata de generar conocimiento mediante la identificación de patrones y gracias al uso de métodos como algoritmos estadísticos, *machine learning* o el análisis de textos. Se centra en el descubrimiento de propiedades desconocidas de los datos entrantes. Se trata de un análisis automático o semiautomático enfocado a amplios conjuntos de datos.

Existen principalmente dos tipos de algoritmos de estructuración de conjuntos de datos dependiendo de la técnica de aprendizaje empleada: algoritmos de clasificación (aprendizaje supervisado) y de agrupamiento o *clustering* (aprendizaje no supervisado).

Los algoritmos de clasificación tienen por objetivo determinar la categoría a la que pertenece un determinado objeto (es decir, una unidad de dato específica de un problema en particular). Para ello, se elabora un modelo que describe una serie de clases predeterminadas que resultan de un proceso de aprendizaje a partir de un conjunto de datos de entrenamiento. El aprendizaje supervisado asume que toda muestra de entrenamiento pertenece a una clase predeterminada. El modelo construido puede representarse bajo la forma de una fórmula, reglas de clasificación o árboles de decisión, entre otros.

De entre las diversas técnicas empleadas por los algoritmos de clasificación, cabe discernir entre las paramétricas (donde el modelo viene definido por una serie de estadísticos) y las no paramétricas (donde se desconoce la densidad

de los datos entrantes). De entre las técnicas paramétricas cabe señalar la estimación por máxima verosimilitud (*Maximum likelihood estimation* (MLE)), la estimación bayesiana (*Bayes estimator*) o el análisis discriminante; mientras que de entre las no paramétricas destacan el clasificador de k vecinos más próximos (*k-nearest neighbours*), el clasificador bayesiano ingenuo (*Naive Bayes classifier*), las máquinas de vectores de soporte (*Support vector machines* (SVM)), las redes neuronales (*Neural networks*) o los árboles de decisión (*Decision trees*).

Por su parte, los algoritmos de *clustering* son también conocidos como métodos semi-paramétricos. En este caso se habla de aprendizaje no supervisado puesto que, a diferencia de los algoritmos de clasificación, se basan en el desconocimiento a priori del modelo de los datos o de la distribución que siguen.

De entre las técnicas de *clustering* más relevantes, cabe destacar el agrupamiento k-medias (*k-means clustering*), el agrupamiento jerárquico (*Hierarchical clustering*), el agrupamiento de correlación (*Correlation clustering*) o el análisis de componentes principales (*Principal Component Analysis* (PCA)).

Más allá de los algoritmos de clasificación o *clustering*, existen otras técnicas de análisis de datos como la regresión (proceso estadístico para la estimación de la relación entre variables dependientes e independientes), los algoritmos de *sequence labelling* (para la predicción de evoluciones), el procesado del lenguaje natural y *text mining* (muy útiles en el área de la inteligencia y la adquisición de información) o el análisis de redes sociales que, basándose sobre todo en la teoría de grafos, busca extraer conocimiento acerca del comportamiento o actividades de una determinada estructura social (detección de comunidades, predicción de conexiones, identificación de actores prominentes y reacciones en cascada son algunas de sus principales utilidades).

En lo que a herramientas para el análisis y minería de datos se refiere, existe en la actualidad un amplio abanico de excelentes soluciones que implementan los anteriores algoritmos y técnicas analíticas. De entre las alternativas *open source* existentes, destacan las siguientes:

- **R Project** [177]: completo paquete de análisis estadístico con cientos de extensiones para *data mining*, *machine learning*, etc.
- **Python** [178]: la tendencia actual ubica a Python como la plataforma *open source* de facto para la computación científica y matemática.
- **Matlab** [179]: pese a tratarse de un entorno de software propietario, muchas de sus bibliotecas y paquetes son fácilmente migrables a Octave, su versión de libre uso.

- **RapidMiner** [180]: evolución comercial de YALE (*Yet Another Learning Environment*), una completa *suite* de minería de datos y análisis predictivo.

Respecto a soluciones comerciales o de licencia propietaria, más allá de Matlab [179] y entre muchas otras, resultan interesantes las siguientes:

- **IBM SPSS Statistics** [181]: paquete estadístico muy extendido en áreas como las ciencias sociales.
- **TIBCO Statistica** [182]: paquete estadístico orientado a operaciones de búsqueda, *data mining* y *business intelligence* en el ámbito de la empresa.
- **Wolfram Mathematica** [183]: solución para el análisis y la minería de datos orientado a la computación técnica, muy extendido en el ámbito académico.
- **Algolytics AdvancedMiner** [184]: *suite* analítica profesional con múltiples herramientas para transformación de datos, modelos de *data mining* o generación de reportes.

Sin embargo, en lo que concierne al ámbito de la inteligencia en particular, resulta difícil hallar herramientas específicas orientadas a tal fin. De entre las soluciones que más se aproximan como Palantir [185], CASOS [186] o Sentinel Visualizer [187], destaca por encima de todas IBM i2 Analyst's Notebook [188]: una completa *suite* de la compañía IBM orientada a la comunidad de Inteligencia que cuenta con módulos específicos para la importación de datos, la gestión de base de datos, el análisis y minería de datos, el análisis de redes sociales y la generación de grafos.

Análisis y evaluación de riesgos

En el campo de los sistemas de información, se habla de análisis de riesgos para referirse al proceso sistemático consistente en estimar la magnitud de los riesgos a los que está expuesta una organización [189], entendiéndose por riesgo:

"The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization."

La evaluación del nivel de riesgo puede por tanto expresarse como una función, a evaluar por cada par 'amenaza identificada/vulnerabilidad existente', que depende de dos variables [190]:

- **Probabilidad**: grado de verosimilitud de que una determinada amenaza explote una determinada vulnerabilidad.
- **Impacto**: magnitud del daño que pueda causar la explotación de una determinada vulnerabilidad por parte de una determinada amenaza.

Donde el impacto (o consecuencias) de los riesgos suele estimarse como el nivel de degradación percibido en cada una de las dimensiones tradicionales que conforman la seguridad de la información, también conocida como tríada *Confidentiality, Integrity and Availability* (CIA) [189]:

- **Confidencialidad**: que la información esté únicamente disponible para las personas, entidades o procesos autorizados.
- **Integridad**: que los datos se mantengan completos y correctos, no siendo alterados o destruidos sin autorización.
- **Disponibilidad**: que en todo momento los datos se hallen accesibles y los servicios operativos para su uso.

A estos canónicos atributos de seguridad de la información, se han ido incorporando otros más recientemente como la autenticidad (que una entidad sea quien dice ser, garantizando así el origen de los datos) o la trazabilidad (que se pueda determinar quién llevó a cabo qué acciones y en qué momento).

Sin embargo, el análisis y la evaluación de los riesgos no son más que las etapas intermedias del conocido como proceso de gestión de riesgos, un concepto todavía más amplio y habitualmente descrito en cuatro fases (Figura 2.14) [191][192]:

1. **Identificación de riesgos**: definición de los riesgos y de las relaciones entre los posibles puntos de peligro. Incluye la identificación de las amenazas y de las vulnerabilidades.
2. **Análisis de riesgos**: calificación de los riesgos identificados de acuerdo tanto a sus potenciales consecuencias (análisis cuantitativo) como a su importancia relativa (análisis cualitativo). Se determina la severidad y probabilidad de ocurrencia de cada evento de riesgo.
3. **Evaluación de riesgos**: clasificación de riesgos por prioridad. Se aplican reglas analíticas de decisión para ordenar los riesgos existentes de mayor a menor criticidad y determinar cuáles resultan aceptables para una organización y cuáles no.

4. **Control de riesgos**: aplicación de planes de mitigación para eliminar o reducir el nivel de riesgo de aquellos considerados como no aceptables. Monitorización continua del plan de mitigación para valorar su eficacia y ajustar el curso de las acciones si fuese necesario.

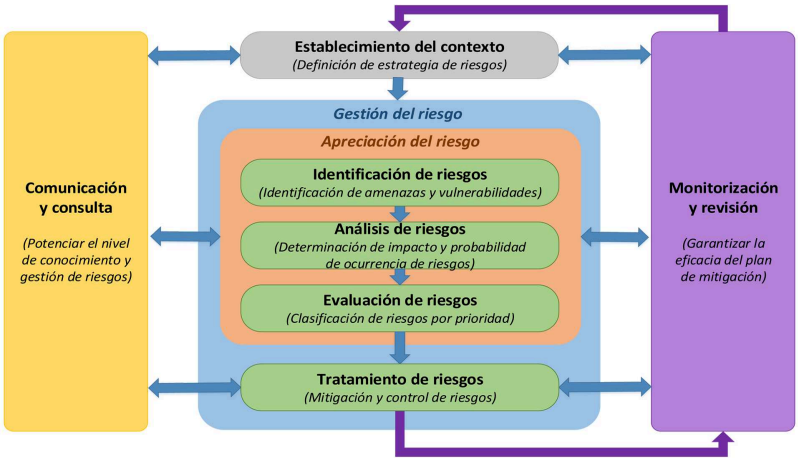


Figura 2.14: Gestión de riesgos (ISO 31000:2009) [13].

En [193], se lleva a cabo una comparativa entre cuatro de las metodologías de gestión de riesgos más relevantes: (i) *Méthode Harmonisée d'Analyse des Risques* (MEHARI) [194]: un método de análisis y gestión de riesgos desarrollado por el *Club de la Sécurité des Systèmes d'Information Français* (CLUSIF), (ii) Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT) [195]: la metodología de análisis y gestión de riesgos para sistemas de información del antiguo Consejo Superior de Administración Electrónica (CSAE) de España, (iii) SP 800-30 [196]: una guía de gestión de riesgos para las TIC elaborada por el NIST y (iv) *Security Risk Management Guide* [197]: una guía de gestión de riesgos de seguridad desarrollada por Microsoft. Los autores determinan que no existe un estándar que defina en detalle las etapas de la gestión de riesgos en la seguridad de la información. Además, concluyen que todas las metodologías estudiadas abarcan las tres primeras fases de la gestión de riesgos e incluyen guías detalladas para el análisis de los mismos; sin embargo solo la del NIST incluye también recomendaciones para el control de riesgos y documentación adicional para la evaluación de estos.

[13] *Risk management - Principles and guidelines*, International Organization for Standardization (ISO), ISO 31000:2009, Nov. 2009.

Cabe por último destacar, a nivel nacional, PILAR [170] como la herramienta desarrollada por el CCN-CERT [18] para el análisis y gestión de riesgos que sigue la metodología MAGERIT [198].

2.4.4. Técnicas de visualización de información

Si bien el análisis de datos tiene como objetivo la obtención de información útil a partir de amplios y complejos conjuntos de datos, la visualización de la información explota el conocimiento previo adquirido y contribuye a incrementar la cognición humana mediante una exploración visual y una eficiente interacción con la información representada [199]. Al emergente campo de estudio que, con el fin de mejorar el proceso de toma de decisiones, combina las ventajas que ofrecen ambos enfoques se le conoce como *visual analytics* [200][201][202].

La *IEEE Visualization Conference* (VIS) [203], que aúna la *IEEE Conference on Visual Analytics Science and Technology* (VAST) [204], la *IEEE Information Visualization Conference* (InfoVis) [205] y la *IEEE Scientific Visualization Conference* (SciVis) [206], constituye el congreso más importante y la principal referencia a nivel mundial para la investigación en el ámbito de la visualización científica y de la información. Especialmente orientado al campo de la ciberseguridad, cabe destacar, como evento celebrado en paralelo al IEEE VIS, el *IEEE Symposium on Visualization for Cyber Security* (VizSec) [207].

A continuación, se presentan con más detalle las principales técnicas de visualización de la información en sistemas SA y, en particular, las actuales tendencias en lo que a la representación de CySA se refiere.

Sistemas GIS y georreferenciación

Los sistemas de información geográfica (*Geographic Information System* (GIS)), inicialmente orientados a la representación georreferenciada y en tiempo real de información espacial, siguen constituyendo hoy en día el componente esencial de casi todo sistema C2IS.

En la actualidad, el mercado ofrece un amplísimo abanico de herramientas GIS para todo tipo de aplicaciones: soluciones GIS comerciales (ArcGIS, Luciad, Carmenta, etc.), de código abierto (QGIS), servidores de mapas (GeoServer, MapServer, etc.), servicios de *web mapping* propietarios (Google Maps, Bing Maps) y de libre uso (OpenStreetMap), *frameworks* para aplicaciones geoespaciales en web (Cesium, OpenLayers, CartoDB, etc.), y muchas más.

Véase, a continuación, una breve descripción de algunas de las propuestas GIS más destacadas.

- **Luciad**

  Luciad [208] nace en 1999 como una *spin-off* de la Universidad de Leuven inicialmente orientada al desarrollo de sistemas de información para la gestión y control del tráfico aéreo. Su filosofía parte de la necesidad de desarrollar capacidades de visualización que integren y fusionen múltiples fuentes de información geoespacial en una COP conjunta. Luciad no comercializa productos finales per se, sino componentes software para el desarrollo de aplicaciones geoespaciales adaptadas a las necesidades del cliente, entre los que destacan: *LuciadLightspeed* (potente *Application Programming Interface* (API) modular, buque insignia de la compañía, orientada al desarrollo de aplicaciones de visualización de datos en tiempo real y sistemas C2) [209], *LuciadRIA* (para el desarrollo de aplicaciones en entorno web) [210], *LuciadFusion* (para gestionar y servir datos geoespaciales de diversas fuentes de información) [211] y *LuciadMobile* (para la creación de aplicaciones móviles) [212]. Erigida hoy en día en líder mundial de soluciones GIS de altas prestaciones, Luciad se halla especialmente presente en sectores como la aviación, la seguridad y sobretodo Defensa (70 % de su clientela) colaborando con empresas y organizaciones como OTAN, Airbus, Boeing o Thales, entre otras.

- **ESRI ArcGIS**

  Con más de cuarenta años de antigüedad, *Environmental Systems Research Institute* (ESRI) nace como un grupo de investigación enfocado en el análisis de información geográfica para tareas de consultoría del territorio. *MapObjects*, lanzada en 1996, representó la primera plataforma de publicación de mapas en Internet. Orientada hoy en día al sector empresarial, ESRI comercializa una *suite* de soluciones GIS [213] que incluye *ArcGIS* como plataforma de *mapping* basada en la nube, aplicación *ArcGIS* para escritorio, ESRI *CityEngine* y ESRI *MapStudio*, entre otras además de *ArcGIS Explorer Desktop*, como visor GIS gratuito. El portal web para desarrolladores de ESRI incluye acceso a las APIs y *Software Development Kit* (SDK)s de ArcGIS, amplia documentación, *live demos* y ejemplos de código. ESRI constituye una de las empresas líder del sector y con mayor experiencia, estando hoy en día presente en más de 350.000 organizaciones de todo el mundo.

- **Carmenta**

  Carmenta [214] es una compañía con más de treinta años de experiencia en el desarrollo de sistemas de alta SA orientados a misiones críticas como la gestión de emergencias, operaciones militares o el control de tráfico. En el centro de su oferta tecnológica se halla Carmenta *Engine*, un motor de

generación de mapas multiplataforma para Windows, Linux y Android cuyo potente SDK soporta el uso de múltiples entornos de desarrollo como .NET, Java o C++. De entre sus principales características, destacan la compatibilidad con más de setenta formatos de datos geográficos que siguen los estándares *Open Geospatial Consortium* (OGC), la renderización por aceleración de hardware de modelos del terreno y el procesado asíncrono y en paralelo de los datos.

- **Google Maps**

  Tras más de diez años de actividad, Google sigue siendo el líder indiscutible en lo que a mapas digitales se refiere a través de su herramienta Google *Maps* [215]. Más allá de aplicaciones para escritorio y dispositivos móviles, cuenta con una amplia gama de interfaces de programación de soluciones entre las que se incluyen Google *Web Services*, Google *Places* o Google *Maps Image*. La compañía proporciona documentación muy detallada de sus APIs así como ejemplos de código, bibliotecas y paquetes de herramientas de desarrollo (SDK).

- **Microsoft Bing Maps**

  Microsoft *Bing Maps* [216] constituye una plataforma de *mapping* muy extendida aunque todavía muy por detrás de Google *Maps*. De entre las funcionalidades y mejoras incorporadas recientemente al sistema, cabe destacar la inclusión de múltiples ciudades en modo *Streetside*, imágenes aéreas en alta resolución en los mapas de *Bing* y nuevas ciudades en modo 3D en la aplicación *Bing Maps Preview*. La documentación de su API resulta muy completa y detallada e incluye un interesante SDK interactivo que ofrece muestras de sus funcionalidades y ejemplos de código para los desarrolladores de aplicaciones JavaScript.

- **OpenStreetMap**

  OpenStreetMap [217] es un proyecto colaborativo para la libre creación y distribución de datos y mapas geográficos. El API de OpenStreetMap no consiste en embeber un mapa pre-elaborado en web, sino que recoge datos georreferenciados en bruto y/o los almacena en su base de datos. La exhaustiva información relativa a la documentación de su API puede encontrarse en la Wiki de OpenStreetMap. La plataforma representa características físicas como por ejemplo edificios comerciales o vías férreas mediante el uso de etiquetas, donde cada etiqueta describe un atributo geográfico.

- **Cesium**

  Cesium [218] es una potente biblioteca *open source* JavaScript de uso gratuito para el diseño de mapas 2D/3D en entornos web que hace uso de WebGL para la renderización de gráficos en 3D. Las principales fortalezas de Cesium.js son la interoperabilidad con diversas fuentes de mapas como Google *Maps*, Microsoft *Bing Maps* u OpenStreetMap; así como la multiplicidad de tipos de datos soportados tales como información del terreno, imágenes, datos vectoriales o modelos 3D. Respecto a este último, Cesium ha implementado recientemente 3D-Tiles, un formato *open source* de datos 3D muy eficiente capaz de transmitir rápidamente ingentes cantidades de datos heterogéneos a través de Internet. Además, existen multitud de *plugins* integrables en Cesium que permiten dotar a este de funcionalidades extra.

- **OpenLayers**

  OpenLayers [219] es una biblioteca *open source* JavaScript que implementa características de HTML5 como WebGL o Canvas 2D para el renderizado de mapas en navegadores web. OpenLayers es capaz tanto de consumir *tiles* de múltiples fuentes de mapas como Microsoft *Bing Maps*, OpenStreetMap, MapQuest, etc. así como de renderizar múltiples formatos de datos geográficos. La web de OpenLayers incluye una galería con una amplia selección de *live demos* y códigos de ejemplo disponibles en el repositorio GitHub. Su API constituye una biblioteca de *mapping* muy popular gracias a su licencia de software libre y su capacidad de interacción con otros proveedores de mapas.

- **CartoDB**

  CartoDB [220] es un motor de análisis y visualización de mapas *open source* orientado al desarrollo de aplicaciones geoespaciales web y móviles. CartoDB proporciona una biblioteca JavaScript (CartoDB.js), diversas APIs y un editor cuya intuitiva interfaz permite la rápida creación de mapas y visualización de datos. La documentación de todas sus herramientas está muy bien organizada y es fácil de seguir. Una de las características más relevantes de CartoDB es *Torque*, una visualización animada que muestra la evolución de los datos geolocalizados a lo largo del tiempo. La popularidad de CartoDB ha crecido sin cesar desde su reciente aparición habiendo convencido ya a clientes tan importantes como NASA, Twitter o The Guardian UK.

La representación georreferenciada de la información consiste en la visualización en mapas 2D/3D de todo tipo de datos (recolectados o almacenados en base de datos) que presenten atributos geográficos. Existen principalmente dos enfoques para el almacenamiento y representación de datos geográficos en un GIS:

- **Datos *raster***: corresponde al valor (asociado a un determinado atributo geográfico como elevación, desnivel, etc.) de las celdas (o píxeles) resultantes del mallado de una imagen digital en una cuadrícula regular.

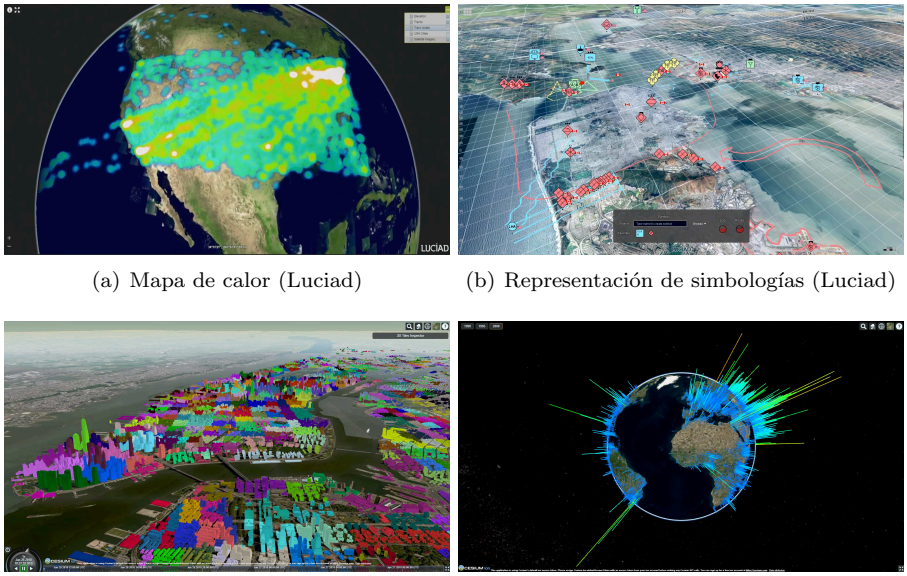
- **Datos vectoriales**: consiste en la representación vectorial (vértices y rutas) de la componente espacial de los datos geográficos mediante puntos, líneas y polígonos como geometrías primitivas.

En lo que a formatos de datos *raster* se refiere, cabe citar JPEG 2000 y otros propietarios como *Enhanced Compression Wavelet* (ECW), GeoTIFF o ESRI *Grid*.

Respecto a datos vectoriales, destacan formatos propietarios como ESRI *Shapefile*, otros basados en *JavaScript Object Notation* (JSON) como Cesium *CZML* o GeoJSON/TopoJSON, así como *eXtensible Markup Language* (XML) o *Geography Markup Language* (GML) entre los definidos por la OGC, un organismo internacional (anteriormente conocido como OpenGIS) que promueve la estandarización en abierto de contenidos y formatos geoespaciales.

En la actualidad, los sistemas GIS y servicios de *web mapping* más completos integran, además de funcionalidades clásicas como la representación de simbologías, herramientas geométricas (cálculo de distancias, perfil del terreno, etc.) o la gestión de la información por capas, avanzadas técnicas de *visual analytics* que abarcan desde grafos georreferenciados hasta la inclusión de la "cuarta dimensión" (evolución temporal de los datos) pasando por la codificación de la información representada por densidad (mapas de calor), color y/o tamaño (objetos volumétricos).

En la Figura 2.15 pueden verse algunos ejemplos de estas representaciones en Luciad y Cesium extraídos de sus respectivas webs.



(a) Mapa de calor (Luciad)

(b) Representación de simbologías (Luciad)

(c) Codificación por color (Cesium)

(d) Codificación por tamaño y densidad (Cesium)

Figura 2.15: Técnicas de georreferenciación de la información [14].

Grafos y diagramas

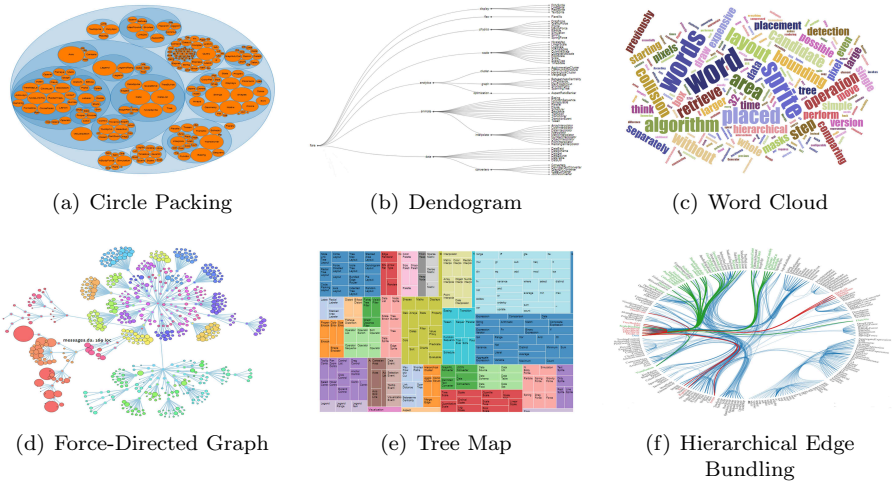
Más allá de mapas y datos georreferenciados, la representación mediante grafos, tanto convencionales como interactivos, constituye otra de las principales técnicas de visualización de la información (física y/o ciber) en el ámbito de la seguridad [221][222][223][224].

Por una parte, aparecen bibliotecas como Microsoft Chart Controls [225], Chart.js [226] o JpGraph [227] orientadas a la obtención de gráficas más tradicionales como *bar charts*, *line charts*, *area charts*, *pie/doughnut charts* o *polar/radar charts*, entre otras.

Por otra parte, han ido surgiendo recientemente interesantes herramientas para la generación de atractivos grafos interactivos entre las que cabe señalar Three.js [228], JavaScript InfoVis Toolkit [229] o, sobretodo, Data-Driven Documents [230], una biblioteca JavaScript de código abierto que emplea HTML, *Scalable Vector Graphics* (SVG) y CSS para generar, a partir de conjuntos de

[14] (a) & (b) Luciad Company, `http://www.luciad.com/videos` [Accessed Apr. 23, 2018].
(c) & (d) Cesium, `https://cesiumjs.org/Cesium/Apps/Sandcastle` [Accessed Apr. 23, 2018].

datos complejos, visualizaciones avanzadas que ofrecen al usuario una fantástica interactividad (Figura 2.16).



(a) Circle Packing (b) Dendogram (c) Word Cloud

(d) Force-Directed Graph (e) Tree Map (f) Hierarchical Edge Bundling

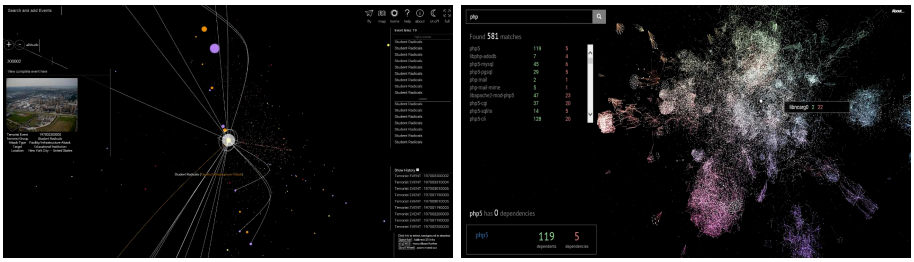
Figura 2.16: Grafos y diagramas interactivos [15].

Algunas de las representaciones más destacadas de la biblioteca D3.js son:

- **Bubble Chart**: codifica datos en el área de circunferencias, por tamaño y color.
- **Circle Packing**: diagrama de agrupamiento que enfatiza las jerarquías entre conjuntos.
- **Dendrogram**: diagrama jerárquico de nodos y vértices en forma de árbol.
- **Force-Directed Graph**: diagrama de nodos y vértices que emplea un algoritmo de posicionamiento que minimiza el cruce de vértices.
- **Tree Map**: mapa generado por subdivisión recursiva donde el valor de cada nodo viene dado por el área de su rectángulo.
- **Hierarchical Edge Bundling**: red de nodos que resalta los enlaces entrantes (dependientes) y salientes (dependencias).
- **Word Cloud**: codifica por tamaños la ocurrencia de las palabras más frecuentes en un texto.

[15] Data-Driven Documents, `https://d3js.org` [Accessed Jul. 23, 2018].

Cuando la cantidad de información a representar es tal que el espacio bidimensional resulta insuficiente para la adecuada interpretación de la misma, las representaciones en 3D resultan la mejor alternativa. En esta línea, algunos de los trabajos más recientes (Figura 2.17), apoyados en la teoría de grafos y de la complejidad, aprovechan las ventajas que ofrece un entorno de representación tridimensional para la visualización interactiva de amplias y complejas redes de datos (no necesariamente georreferenciados) [231][232].



(a) Proyecto *WikiGalaxy* (b) Proyecto *Code Galaxies*

Figura 2.17: Representaciones tridimensionales de datos complejos [16].

Pueden encontrarse en la red multitud de webs, foros o repositorios en los que los usuarios publican y comparten ejemplos de aplicación de *visual analytics* en trabajos y proyectos de todo tipo de disciplinas [233][234][235][236].

Por último, aparecen también en el mercado diversas herramientas comerciales como Tableau [237], Datawrapper [238] o Infogram [239] que se presentan como alternativas interesantes en el ámbito de la visualización de la información mediante grafos.

Visualización inmersiva

En los últimos años, han ido adquiriendo cada vez más relevancia técnicas de visualización inmersiva como la realidad aumentada (*Augmented Reality* (AR)) o la realidad virtual (*Virtual Reality* (VR)) para la representación de información en el ámbito de la seguridad [240].

Tal y como comentado anteriormente, la proyección de visualizaciones 3D en planos 2D conlleva a menudo problemas de superposición de la información que podrían evitarse al distribuir las conexiones (relaciones) entre nodos (entidades) entre las tres dimensiones [231]. En particular, la VR constituye un entorno

[16] (a) WikiGalaxy Project, `http://wiki.polyfra.me` [Accessed Jul. 23, 2018].
(b) Code Galaxies Project, `https://anvaka.github.io/pm` [Accessed Jul. 23, 2018].

natural para la visualización de grafos 3D que mejora la consciencia situacional del usuario al permitirle navegar e interactuar de manera más intuitiva entre estructuras complejas de datos.

La amplia y variada oferta del mercado en cuanto a visores de VR, también llamados cascos estereoscópicos (*Head-Mounted Displays* (HMD) y *Head-Coupled Displays* (HCD)), distingue dos principales tipos de dispositivos [241] (cuyas principales características y productos vienen resumidos en la Tabla 2.6): dispositivos VR *tethered* (conectados físicamente al PC) y dispositivos VR móviles (integrados directamente con el *smartphone*).

	VR *tethered*	**VR móvil**
Ventajas	• *Tracking* de movimiento muy preciso (sensores externos (6-DoF*)) • Mayor fidelidad de imagen (visor dedicado)	• Mayor comodidad y libertad de movimiento • No requiere ningún hardware adicional • Precios económicos
Inconvenientes	• Menor confortabilidad (debido al cableado) • Requiere PCs de altas prestaciones • Precios elevados	• *Tracking* de movimiento menos preciso (3-DoF*) • Limitada calidad de imagen (la nativa del dispositivo móvil)
Productos destacados	• Oculus Rift [242] • HTC Vive [244]	• Samsung Gear VR [243] • Google Daydream [245]

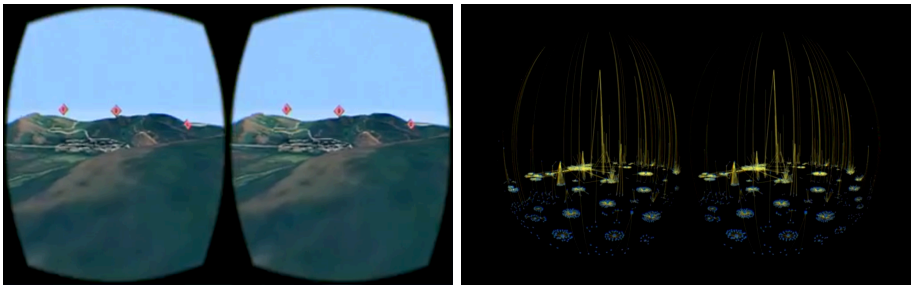
*DoF (*Degrees of Freedom*): grados de libertad.

Tabla 2.6: Tipos de dispositivos de VR y sus características.

Las propuestas más novedosas en este campo se encaminan ahora hacia dispositivos independientes de VR como alternativa a los visores VR móviles pero sin necesidad del dispositivo móvil en sí (Oculus Go [246], Lenovo Mirage Solo [247], etc.); así como hacia soluciones de realidad mixta que integran capacidades tanto de VR como de AR en un mismo dispositivo (Samsung Odyssey [248], Microsoft Windows Mixed Reality [249], etc.).

La visualización inmersiva mediante VR puede aplicarse, entre muchas otras, a las diferentes técnicas de representación anteriormente presentadas. En efecto, soluciones GIS como Luciad o Cesium soportan ya dispositivos VR como Oculus Rift [242] a través de desarrollos en LuciadLightspeed o *plugins* como Cesium-VR/Cesium-Leap [250][251] respectivamente (Figura 2.18(a)). Además, la compañía Oculus [252] ha encontrado un socio estratégico fundamental en Unity [253], una plataforma para el desarrollo de escenas y contenidos

interactivos 3D. Mediante estas, resulta posible el diseño de entornos inmersivos para la representación y navegación entre, por ejemplo, complejos grafos o estructuras de datos tridimensionales (Figura 2.18(b)) [232].



(a) Oculus Rift & LuciadLightspeed (b) Oculus Rift & Unity

Figura 2.18: Ejemplos de visualización inmersiva [17].

[17] (a) Oculus Rift & LuciadLightspeed, `http://www.luciad.com/videos` [Accessed Jul. 6, 2018].
(b) Oculus Rift & Unity, `https://vimeo.com/110246045` [Accessed Jul. 23, 2018].

Capítulo 3

Definición de la arquitectura

3.1. Introducción

En la actualidad, la adecuada protección de las infraestructuras críticas requiere considerar, más allá de las amenazas presentes en el espacio físico, todas aquellas inherentes al ciberespacio. Más aún cuando un ataque a cualquiera de estas dimensiones puede desencadenar efectos cascada sobre todas ellas. Sin embargo, como se ha visto en el capítulo 2, las soluciones existentes hoy en día en este sentido resultan todavía insuficientes. Mientras que los SIEMs por si solos a menudo ofrecen una defensa únicamente preventiva o pasiva y visualizaciones poco intuitivas, las soluciones SCADA más avanzadas [254][255], como subconjunto de los tradicionales ICS, permanecen fundamentalmente orientadas a sectores industriales [256].

El objetivo de este capítulo es, por consiguiente, la presentación de una arquitectura genérica de HSA que, por combinación de las situaciones del dominio físico (PSA) y ciber (CySA) en un único espacio de representación, permita afrontar de manera ágil y eficiente la protección de cualquier tipo de infraestructura en el entorno ciber-físico. El modelo propuesto no es por tanto el de una herramienta de análisis, sino el de una aplicación fundamentalmente de visualización que busca sobreponer las limitaciones de las soluciones actuales de defensa y, mediante técnicas avanzadas de representación, facilitar la toma de decisiones al responsable de seguridad en cuestión.

3.2. Visión general

Diseñada de manera flexible para adaptarse a diferentes entornos de funcionamiento, la arquitectura de HSA propuesta (Figura 3.1) está principalmente compuesta de cuatro módulos independientes, que en posteriores apartados serán descritos con más detalle:

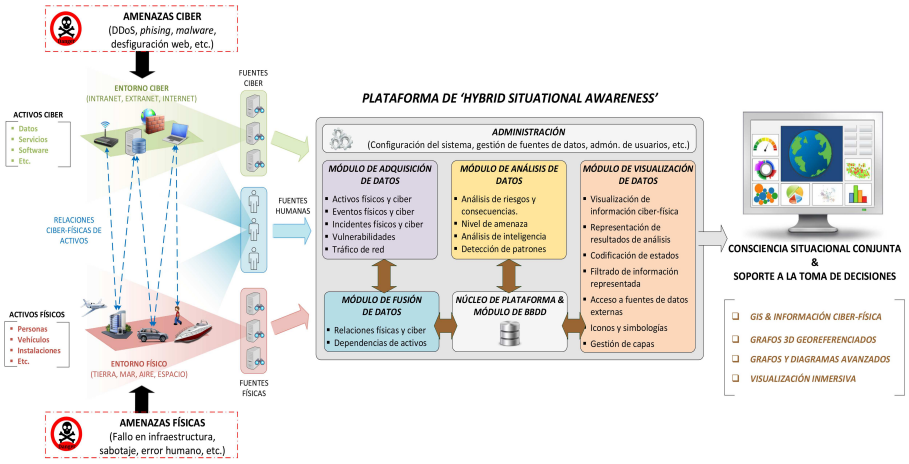


Figura 3.1: Visión general de la arquitectura.

- **Adquisición de datos**

  Es responsable de recolectar, a través de diversas fuentes heterogéneas de datos físicos, ciber o mixtos, toda información relativa a activos, vulnerabilidades, amenazas, eventos o incidentes tanto físicos como ciber.

- **Fusión de datos**

  Es responsable de combinar los datos obtenidos de las diferentes fuentes de datos integradas con el fin de establecer relaciones entre la información de los mundos físico y ciber así como dependencias entre activos.

- **Análisis de datos**

  Es responsable de producir, mediante procesados distintos de los datos según el caso de uso (análisis de riesgos, nivel de amenaza, análisis de inteligencia, detección de patrones, etc.), información de interés que facilite la toma de decisiones en el contexto correspondiente.

- **Representación de información**

  Es responsable de generar, por integración de la PSA y de la CySA en un único espacio de visualización a través de técnicas avanzadas de representación, la adecuada HSA del entorno ciber-físico en su conjunto.

Asimismo, un módulo adicional de administración será el encargado de tareas tales como la configuración general de la plataforma, la configuración de las fuentes de datos, la gestión de usuarios y privilegios, etc.

La presente arquitectura, desarrollada mediante tecnologías y herramientas actuales, ha sido definida en cualquier caso con la intención de facilitar tanto la integración de nuevas funcionalidades como el cumplimiento de futuros requerimientos adicionales.

3.3. Adquisición de datos

La arquitectura que aquí se presenta, ha sido pensada para poder integrar múltiples fuentes de datos relativas tanto al dominio físico como al ciberespacio. Se distinguen principalmente tres tipos en función de las dimensiones en las que actúan: fuentes de datos ciber, físicos o mixtos.

3.3.1. Fuentes de datos ciber

Las fuentes de datos ciber hacen principalmente referencia a dispositivos SIEM que, como se ha visto en el capítulo 2, consisten en avanzados sistemas de seguridad en red que monitorizan en tiempo real los activos ciber (sistemas operativos, ficheros de datos, servicios, software, etc.) existentes en su red a través del análisis y correlación de los datos proporcionados por componentes básicos de seguridad (como *firewalls*, IDS/IPS, antivirus, etc.) desplegados en la misma a modo de agentes o sensores.

Las fuentes de datos de ámbito ciber, tanto SIEMs como otras, por las que se ha optado para la arquitectura propuesta en la presente tesis son las siguientes:

- **OSSIM**

  Esta herramienta gratuita de AlienVault [146] representa la solución SIEM *open source* más completa (Figura 3.2), de mejor reputación y, por ende, una de las más extendidas en diversos sectores. De entre las infinitas funcionalidades que ofrece (colección de *logs*, correlación de eventos, evaluación de riesgos, monitorización de red, etc.), son sus capacidades

de inventariado (descubrimiento de activos en la red), escaneo de vulnerabilidades, análisis de tráfico y gestión de alarmas las que resultan de mayor interés para el modelo propuesto.

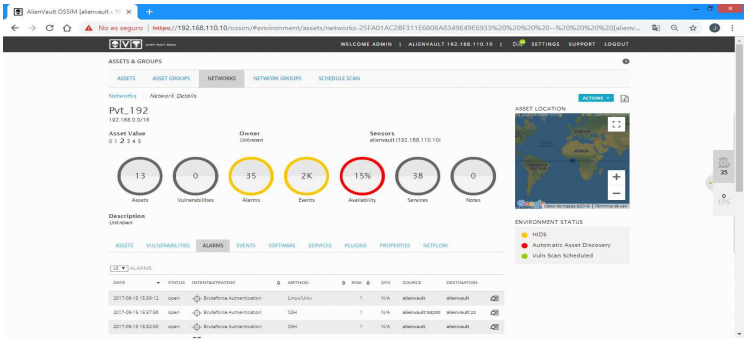


Figura 3.2: Vista de la interfaz de OSSIM.

- **MISP**

  Con el fin de completar las capacidades que ofrece OSSIM, se propone la integración de MISP [156][257] como plataforma de libre uso y gratuita para de intercambio de información de amenazas ciber e indicadores de compromiso de objetivos de ataques (Figura 3.3). A diferencia de los SIEMs, es capaz de recopilar información en formatos no estructurados y está disponible para ser usada por personal no necesariamente especializado. Para la presente arquitectura, se hará uso de toda información de amenaza o evento de seguridad que esta pueda proveer.

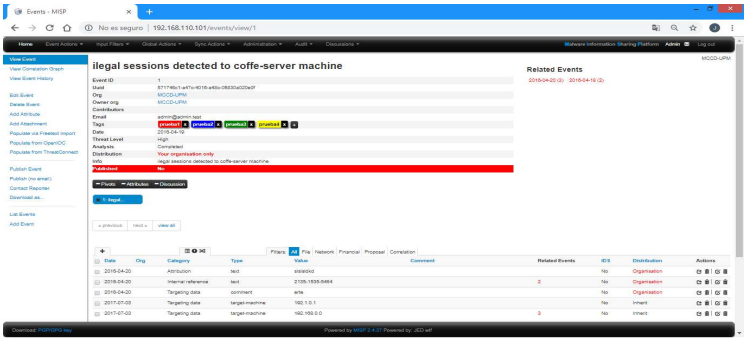


Figura 3.3: Vista de la interfaz de MISP.

- **RTIR**

  De manera complementaria a las soluciones anteriores, se sugiere la utilización de la plataforma *open source* de *ticketing* RT y, en particular, su distribución específica para el seguimiento e intercambio de información de ciberincidentes, RTIR [157], desarrollada a partir de las necesidades de equipos *Computer Emergency Response Team* (CERT) (Figura 3.4). También gratuita y de sencillo uso para cualquier usuario, resulta de utilidad para la arquitectura propuesta por la información detallada que ofrece de todo evento ciber declarado como incidente.

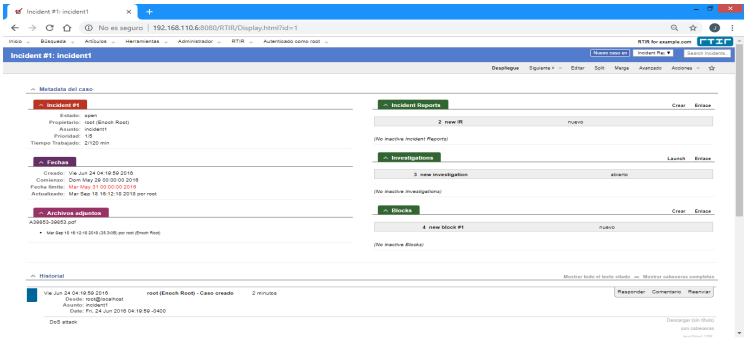


Figura 3.4: Vista de la interfaz de RTIR.

Si bien estas tres plataformas constituyen el núcleo común de fuentes de datos ciber, la arquitectura diseñada está preparada para la fácil integración de herramientas adicionales. De este modo, en caso de aplicar la arquitectura definida a un sistema de ciberseguridad, se propone también:

- **PILAR**

  Se trata de la solución del CCN-CERT para el análisis y gestión de riesgos en diversos tipos de sistemas de información. Siguiendo la metodología MAGERIT, PILAR [170] está pensada para un análisis estático en grandes redes de activos ciber, evaluando el riesgo en cada una de las dimensiones de seguridad de la información: confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad.

3.3.2. Fuentes de datos físicos

Puesto que la arquitectura de HSA que aquí se expone pretende ser lo suficientemente genérica para ser aplicable a cualquier tipo de entorno o infraestructura, se ha optado por no integrar de inicio ningún tipo de fuente de datos de ámbito físico al modelo propuesto, quedando abierta la elección de las mismas para cada caso de uso en particular.

En cualquier caso, cabe indicar que este tipo de fuentes de datos hacen principalmente referencia a todo tipo de sensor desplegado en cualquiera de las dimensiones del espacio físico (tierra, mar, aire o espacio) con la finalidad de monitorizar el estado de los activos físicos (personas, vehículos, inmuebles, instalaciones, etc.) presentes en la misma y alertar de cualquier evento anormal o incidente detectado.

Estas fuentes de datos físicos pueden por tanto abarcar desde sensores ambientales hasta dispositivos GPS, detectores de presencia, *smartcards* con tecnología RFID o cámaras de videovigilancia en CCTV, entre muchas otras.

3.3.3. Fuentes de datos mixtos

Se entiende por fuentes de datos mixtos todas aquellas que, de un modo u otro, proporcionan datos relativos tanto al dominio físico como al ciberespacio. En el caso particular de la presente tesis, estas hacen referencia directa a la inteligencia humana o HUMINT, es decir, a toda información útil relativa a cualquiera de estas dimensiones que deriva de los datos proporcionados por medios humanos.

Este tipo de fuentes resulta especialmente interesante en el caso de un sistema avanzado de inteligencia donde la información, tanto de dominio físico como ciber, proporcionada por todo usuario autorizado (ya sea desde un simple informador hasta un agente de seguridad o analista de inteligencia) puede resultar clave, en combinación con la obtenida por otros medios, para alcanzar una adecuada y completa consciencia situacional y, por ende, una correcta toma de decisiones.

A modo de ejemplo, la información de inteligencia que este tipo de fuentes podría proporcionar incluye, entre muchas otras, la observación directa de eventos relevantes, el reconocimiento visual del acceso de intrusos, el reporte de todo comportamiento sospechoso o inusual, etc.

La Tabla 3.1 recoge, de manera sintética y resumida, las diferentes fuentes de datos que conforman la arquitectura propuesta y la información que cada una de ellas proveerá al modelo.

Ámbito	Caso de uso	Fuente	Información
Ciber	GESTPIC & HYBINT	OSSIM	• Activos ciber • Vulnerabilidades • Tráfico de red
		MISP	• Eventos ciber • Amenazas ciber
		RTIR	• Incidentes ciber
	GESTPIC	PILAR	• Valor de activos • Amenazas de activos • Riesgos de activos
Físico	GESTPIC & HYBINT	Sensores, Cámaras, GPS, etc.	• Activos físicos • Eventos físicos • Incidentes físicos
Mixto	HYBINT	Humana	• Eventos ciber • Incidentes ciber • Eventos físicos • Incidentes físicos

Tabla 3.1: Fuentes de datos de la arquitectura de HSA.

3.3.4. Interoperabilidad

Existen diversas alternativas de interoperabilidad con las diferentes fuentes de datos anteriormente expuestas dependiendo de las posibilidades, tanto en lo que a protocolos de comunicación como a formatos de datos se refiere, que cada una de ellas proporciona.

- **OSSIM**

  En lo que concierne a la plataforma OSSIM, y como se vio anteriormente, AlienVault dispone de OTX [116] como un protocolo propio de libre uso para el intercambio de información de amenazas ciber.

  Además, la compañía publica en su solución SIEM comercial (AlienVault USM) una API basada en operaciones *REpresentational State Transfer* (REST) (Figura 3.5) [258]. Toda petición a dicha API devuelve un objeto JSON y un código de respuesta para indicar posibles errores en la comunicación.

```
GET "https://your-subdomain.alienvault.cloud/api/{version}/alarms/{alarmId}" \
    -d @request_body \
    --user username:password
```


```
{
  "uuid": "971918fd-a569-548a-5a80-1ffcda2a8365",
  "has_alarm": false,
  "needs_enrichment": true,
  "priority": 20,
  "rule_intent": "Environmental Awareness",
  "app_type": "amazon-aws",
  "source_username": "user@alienvault.com",
  "destination_name": "ec2.amazonaws.com",
  "timestamp_occured": "1517932134000",
  "authentication_type": "IAMUser",
  "event_type": "Alarm",
  "rule_method": "AWS EC2 Security Group Modified",
  "priority_label": "low",
  "app_id": "amazon-aws",
  "source_name": "x.xx.xx.xxxx",
  "timestamp_received": "1517933139670",
  "rule_strategy": "Network Access Control Modification",
  "timestamp_received_iso8601": "2018-02-06T16:05:39.670Z",
  "request_user_agent": "signin.amazonaws.com",
  "rule_id": "AWSEC2SecurityGroupMod",
  "timestamp_occured_iso8601": "2018-02-06T15:48:54.000Z",
  "event_name": "Add inbound network traffic rule to security group",
  "status": "open"
}
```


Figura 3.5: Ejemplo de API web AlienVault.

De manera sintética, se puede definir REST [259] como una tecnología que implementa una arquitectura orientada a servicios (*Service-Oriented Arquitecture* (SOA)) para el intercambio de datos en múltiples formatos (texto, XML, JSON, binarios, etc.) mediante el protocolo *Hypertext Transfer Protocol* (HTTP) haciendo uso tanto de sus códigos de respuesta nativos como de su conjunto de operaciones, de las cuales destacan principalmente cuatro: *GET* (LEER), *POST* (CREAR), *PUT* (EDITAR) y *DELETE* (ELIMINAR).

- **MISP**

La plataforma MISP dispone, por su parte, de *PyMISP* [260] como una API igualmente basada en REST. Se trata en este caso de una biblioteca gratuita y de código abierto desarrollada en lenguaje Python [178]. Esta API sigue el estándar *Structured Threat Information eXpression* (STIX) [112] de Mitre como lenguaje estructurado para el intercambio de información de ciberamenazas, y los objetos devueltos pueden solicitarse tanto en formato XML como en formato JSON (Figura 3.6).

```
GET "Authorization: a4PLf8QICdDdOmFjwdtSYqkCqn9CvN0VQt7mpUUf"
--header "Content-Type: application/json" --header "Accept: application/json"
http://10.50.13.60/attributes/548847db-060c-4275-a0c7-15bb950d210b
```


```
{
    "Attribute": {
        "id": "39",
        "event_id": "1",
        "object_id": "0",
        "object_relation": null,
        "category": "Payload installation",
        "type": "md5",
        "to_ids": true,
        "uuid": "548847db-060c-4275-a0c7-15bb950d210b",
        "timestamp": "1418217435",
        "distribution": "3",
        "sharing_group_id": "0",
        "comment": "Regin samples collected.",
        "deleted": false,
        "disable_correlation": false,
        "value": "049436bb90f71cf38549817d9b90e2da",
        "event_uuid": "54884656-2da8-4625-bf07-43ef950d210b"
    }
}
```


Figura 3.6: Ejemplo de API web MISP.

- **RTIR**

  Los desarrolladores de la herramienta RT han implementado también, bajo la forma de un *plugin* adicional denominado *REST2* [261], su propia API REST, de libre acceso y *open source*, totalmente compatible con la plataforma RTIR a partir de la versión 4.2.4 de RT. Esta admite peticiones con contenido en formato XML o JSON, y devuelve exclusivamente objetos JSON en sus respuestas (Figura 3.7).

```
GET 'Authorization: token XX_TOKEN_XX' 'XX_QUEUE_URL_XX'
```


```
{
   "id" : 1,
   "Name" : "General",
   "Description" : "The default queue",
   "Lifecycle" : "default",
   "CustomFields" : {},
   "_hyperlinks" : [
      {
         "id" : "1",
         "ref" : "self",
         "type" : "queue",
         "_url" : "XX_RT_URL_XX/REST/2.0/queue/1"
      },
      {
         "ref" : "history",
         "_url" : "XX_RT_URL_XX/REST/2.0/queue/1/history"
      },
      {
         "ref" : "create",
         "type" : "ticket",
         "_url" : "XX_RT_URL_XX/REST/2.0/ticket?Queue=1"
      }
   ],
}
```


Figura 3.7: Ejemplo de API web RTIR.

- **Fuentes de datos físicos**

  En lo que a la interoperabilidad con fuentes de datos del mundo físico se refiere, esta dependerá por completo del ámbito de aplicación de la arquitectura aquí propuesta y del tipo de fuentes de datos físicos integradas en cada caso.

```
<?xml version="1.0" encoding="UTF-8"?>
<nvg:nvg  xmlns:xsi='http://www.w3.org/2001/XMLSchema-instance'
   xmlns:nvg='https://tide.act.nato.int/schemas/2012/10/nvg'
   xsi:schemaLocation='https://tide.act.nato.int/schemas/2012/10/nvg ../../Schemas/nvg.2.0.xsd'
   version="2.0.0">
    <nvg:polyline
           label="Enemy line"
           uri="urn:md5:56688b08cf5d9a902786a14791cde933"
           symbol="app6a:GHC*MGAUAE*****"
           style="stroke-width:1;stroke:rgb(100,100,100);"
           points="15.5,60 16,60 16.5,60">
       <nvg:textInfo>Example polyline for documentation</nvg:textInfo>
    </nvg:polyline>
    <nvg:circle
          uri="urn:md5:3d8d413aa68c89cfdsa990b3ebc8f7e89a57"
          label="Styled circle"
          cx="17" cy="60" r="5000"
          style="stroke-width:1;stroke-dash:15;fill:#66ff66;fill-opacity:0.5">
          <nvg:textInfo>Example circle for documentation</nvg:textInfo>
           <nvg:exclude>
              <nvg:linear-ring points="17,60 17.03,59.98 17.03,60.03 17,60.03"/>
           </nvg:exclude>
    </nvg:circle>
</nvg:nvg>
```

Figura 3.8: Ejemplo de petición NVG.

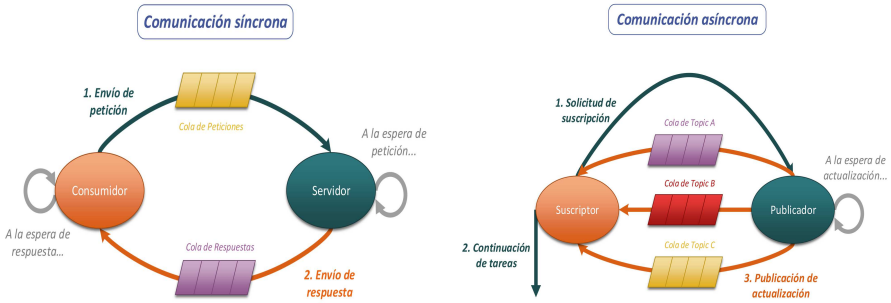
En un entorno táctico, por ejemplo, la comunicación con sistemas C2 suele llevarse a cabo a través del protocolo NVG [262], un estándar desarrollado por OTAN para el intercambio de información de unidades y metadatos basado en SVG [263], un formato de imágenes vectorial descrito en XML (Figura 3.8).

En caso de que una determinada fuente de datos no disponga de una API específica u otros mecanismos propios de interoperabilidad, se tratará de garantizar la comunicación con esta de manera alternativa mediante llamadas REST estándar. Para ello, según las posibilidades de cada fuente y el tipo de comunicación requerida, se optará por alguno de los dos mecanismos de intercambio de mensajes principales (Figura 3.9) [264]: *Request-Response* o *Publish-Subscribe*.

El modelo Petición-Respuesta (*Request-Response*) (Figura 3.9(a)), el más extendido entre los servicios web, es un modo de comunicación síncrono donde el consumidor cursa una petición al servidor, que devuelve la respuesta correspondiente.

El modelo Publicación-Suscripción (*Publish-Subscribe*) (Figura 3.9(b)) es un modo de comunicación asíncrono en el que, mediante un sistema de noti-

ficaciones, el publicador (servidor) informa al suscriptor (consumidor) cuando se producen actualizaciones en aquellos *topics* a los cuales este se ha suscrito.



(a) *Request-Response* (b) *Publish-Subscribe*

Figura 3.9: Mecanismos de comunicación.

3.4. Fusión de datos

3.4.1. Modelo relacional

Puesto que la arquitectura de HSA pretende ser lo suficientemente genérica para adaptarse a diferentes casos de uso en lo que a protección de infraestructuras críticas se refiere, no es posible definir un modelo de datos único y detallado de la misma. Pese a ello, y como elemento clave para la obtención de una adecuada consciencia situacional del espacio ciber-físico, la Figura 3.10 ilustra, de manera simplificada, el esquema de datos propuesto para la fusión de información de fuentes heterogéneas de datos.

Debido a que la generación de la HSA deriva, como comentado anteriormente, de la integración de la CySA sobre la tradicional PSA; el activo ciber se erige, como puede verse en la imagen, en la entidad central del presente modelo, siendo tanto su identificador único (*Globally Unique Identifier* (GUID)) como su dirección IP sus atributos principales y unívocos.

La información en cuestión de dichos activos así como otra relativa a los mismos (vulnerabilidades, flujos de red, propiedades, etc.) es proporcionada por OSSIM y queda relacionada (enlaces azules) automáticamente mediante los identificadores propios de dicha fuente de datos.

Por otra parte, la información relativa a eventos e incidentes ciber, al venir dada por fuentes distintas de datos (MISP y RTIR respectivamente) con sistemas de identificación distintos, queda en este caso directamente vinculada a

los activos ciber correspondientes (enlaces amarillo y rojo respectivamente) a través de la dirección IP de estos.

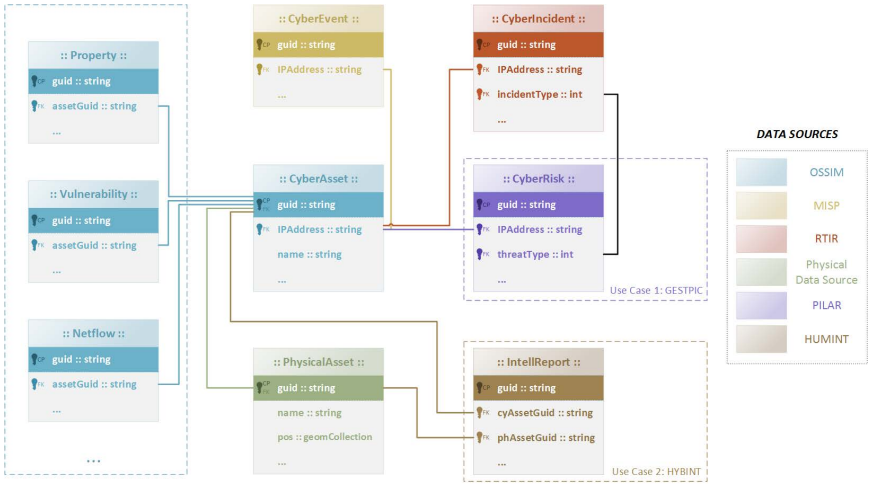


Figura 3.10: Modelo de datos simplificado.

El activo físico incluye, como entidad única relativa al espacio físico y más allá de un identificador unívoco, un atributo específico que determina su localización geográfica. En este caso, corresponde al usuario establecer las correspondientes relaciones (de pertenencia, dependencia, inclusión, etc.) entre activos físicos y ciber (enlace verde). De este modo, información a priori no referenciable geográficamente (como toda la relativa al ciberespacio) resulta ahora geoposicionable a través de estas asociaciones.

Además, en el caso de un sistema de seguridad ciber-física, la información derivada del análisis de riesgos viene dada por PILAR y queda de nuevo directamente relacionada con los activos ciber correspondientes mediante sus direcciones IP (enlace morado). Asimismo, se ha establecido una relación (enlace negro) entre tipologías de amenazas (nomenclatura de PILAR) y tipologías de incidentes (nomenclatura de RTIR) en los que estas pueden derivar.

Por último, en el caso de un sistema avanzado de inteligencia, una entidad adicional recoge toda información de inteligencia proporcionada por los usuarios autorizados. Dicha información, que puede ser relativa tanto al dominio físico como al ciber o a ambos, quedará directamente asociada a los activos afectados a través de sus identificadores propios (enlaces marrones).

3.4.2. Base de datos

En la actualidad, se distinguen dos principales filosofías en lo que a bases de datos se refiere: las bases de datos SQL y las bases de datos NoSQL.

Las bases de datos SQL son bases de datos relacionales desarrolladas en lenguaje *Structured Query Language* (SQL) [265]. Desde su aparición en los años 1970, perseveran como la alternativa principal de almacenamiento de datos; siendo la opción por la que todavía se decantan muchas de las grandes compañías. Cabe mencionar, de entre las diferentes bases de datos SQL, Microsoft SQL Server [266] y Oracle DB [267] entre las de licencia propietaria; mientras que Oracle MySQL [268], de libre acceso y código abierto, permanece como la base de datos más popular a nivel mundial.

Las bases de datos NoSQL [269][270], por su parte, han surgido vertiginosamente en los últimos años como una alternativa a las tradicionales bases de datos relacionales. Diseñadas con el fin de satisfacer las necesidades actuales del *Big Data*, son capaces de almacenar, gestionar y recuperar volúmenes ingentes de datos que siguen modelos de datos dispares. De entre las distintas bases de datos NoSQL, cabe destacar Apache Cassandra [271], Apache HBase [272] y MongoDB [273], siendo todas ellas de licencia abierta.

La Tabla 3.2 muestra, de manera resumida, las principales ventajas que presentan las bases de datos SQL y NoSQL.

	SQL	**NoSQL**
Ventajas	• Uso de lenguaje estándar • Alta compatibilidad • Comunidad muy extensa • Potentes herramientas administrativas	• Orientación a *Big Data* • Escalabilidad elástica • Administración sencilla • Modelos de datos genéricos
Inconvenientes	• Modelos de datos precisos • Flexibilidad limitada • Almacenamiento poco personalizable	• Falta de estandarización • Comunidad limitada • Escasas herramientas de generación de informes

Tabla 3.2: Bases de datos SQL y NoSQL.

Para la arquitectura de HSA aquí propuesta, se ha optado finalmente por la utilización de una base de datos MySQL [268]. La definición de un modelo de datos propio para cada uno de los sistemas presentados permite obviar, en este caso, tecnologías más flexibles como las bases de datos NoSQL; a cambio de aprovechar las diversas ventajas que ofrecen las bases de datos relacionales y,

en particular, MySQL: es ligera, de licencia pública y código abierto, altamente compatible, hace uso de un lenguaje estandarizado (SQL), goza de una amplia comunidad y soporte en línea, dispone de herramientas administrativas muy potentes, etc.

En cualquier caso, se propone igualmente el desarrollo de una capa de abstracción (*Database Abstraction Layer* (DBAL)) que, desacoplando el núcleo del sistema del acceso a base de datos, permita no solo optimizar el rendimiento general de este sino también permitir la integración sencilla en el futuro de motores de base de datos distintos.

3.5. Análisis de datos

Las funcionalidades de análisis y correlación de datos de la arquitectura de HSA aquí presentada dependen por completo del tipo de solución al que se vaya a aplicar la misma.

3.5.1. Análisis de riesgos

En el caso de aplicar la arquitectura genérica de HSA propuesta a una solución de seguridad ciber-física, se entiende fundamentalmente por análisis de datos, el análisis de los riesgos a los que está expuesto el conjunto de activos, tanto físicos como ciber, de la infraestructura en cuestión.

A tal fin, y como comentado en secciones anteriores, se propone la integración y uso de la herramienta PILAR del CCN-CERT. La metodología MAGERIT [198], de la que esta hace uso, consiste a grosso modo en una serie de pasos establecidos (Figura 3.11):

1. Determinar los activos, físicos y ciber, relevantes para la organización (o infraestructura crítica en este caso), sus dependencias y su valor, en el sentido de qué coste supondría su degradación.

2. Determinar a qué amenazas están expuestos aquellos activos.

3. Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo.

4. Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.

5. Estimar el riesgo, definido como el impacto ponderado con la probabilidad de ocurrencia (expectativa de materialización) de la amenaza.

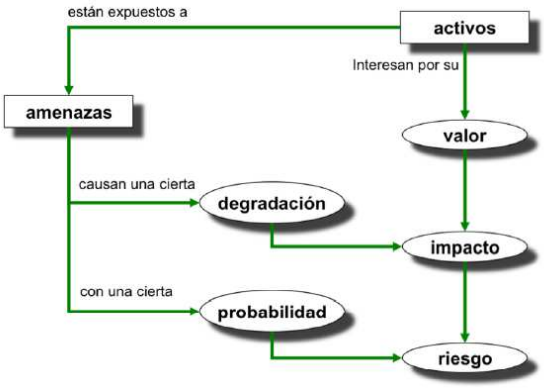


Figura 3.11: Proceso de análisis de riesgos (metodología MAGERIT) [1].

Del análisis de riesgos efectuado por PILAR derivan, a la postre, tres conjuntos de información formateada que serán adquiridos por la plataforma de HSA:

- **Activos**

  La información de activos proporcionada indica, en primer lugar, la tipología de los mismos; distinguiendo entre aquellos esenciales para los sistemas de información (datos y servicios) de otros subordinados a estos (software, hardware, comunicaciones, etc.).

  Las dependencias, por su parte, hacen precisamente referencia a esta interrelación jerárquica entre activos. En otras palabras, los activos vienen a constituir árboles de dependencias en los que la seguridad de los activos "superiores" (esenciales) depende de la seguridad de los activos "inferiores" (subordinados). La interpretación de las rutas que conforman esta estructura depende del sentido en el que se observe: si de arriba a abajo reflejan las dependencias entre activos, de abajo a arriba reflejan las posibilidades de propagación del daño en caso de materialización de amenazas.

  El valor de los activos deriva de cuán necesario es protegerlos y, por ende, del nivel de seguridad que requieren. La valoración de los mismos, que puede ser cualitativa o cuantitativa, se efectúa por cada una de las

[1] *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*, Ministerio de Hacienda y Administraciones Públicas, MAGERIT, Versión 3, Oct. 2012.

dimensiones en las que pueda verse perjudicado el activo ante un incidente y ha de primar criterios de homogeneidad (entre dimensiones) y de relatividad (entre activos). Se habla de valor propio (en el caso de activos "superiores") o acumulado (en el caso de activos "inferiores"), donde estos últimos acumulan el valor de sus superiores.

- **Amenazas**

  La información de amenazas recoge, por su parte, la tipología de las amenazas de las que podría ser víctima cada uno de los activos en cada una de sus dimensiones de seguridad. Por cada una de estas amenazas, se determina la influencia sobre el valor del activo en cuestión a través de dos factores: la degradación del mismo y la probabilidad de ocurrencia.

  La degradación, que representa el daño que causaría la materialización de un incidente, suele expresarse como una fracción del valor total del activo. La probabilidad de ocurrencia, que indica cuán de probable es que se consume una amenaza, puede expresarse tanto mediante una escala nominal como mediante un valor de frecuencia referenciada.

  De todo lo anterior deriva la determinación del impacto potencial, como la medida del daño sobre el activo resultante de la concreción de una amenaza. Tomando en consideración las dependencias entre activos, se habla de impacto acumulado e impacto repercutido. Estos se calculan por cada activo, por cada amenaza y en cada dimensión de valoración en función del valor acumulado (para el impacto acumulado) o propio (para el impacto repercutido), y de la degradación causada (3.1). El impacto es mayor cuanto mayor es: el valor propio del activo (o el acumulado, en el caso del impacto acumulado), la degradación del mismo o también, en el caso del impacto repercutido, la dependencia del activo atacado.

$$Impacto = f(Valor_{Activo}, Degradación_{Activo}) \tag{3.1}$$

- **Riesgos**

  La información de riesgos, por último, hace referencia a las medidas de daño probable sobre un determinado sistema de información. El riesgo potencial, que deriva del impacto de las amenazas sobre los activos y de la probabilidad de ocurrencia de las mismas (3.2), diferencia también entre riesgo acumulado y riesgo repercutido. El riesgo acumulado, que se calcula a través del impacto acumulado (y por ende sobre los activos "inferiores"), refleja las salvaguardas de las que hay que dotar a los activos. El riesgo repercutido, que se calcula a través del impacto repercutido (y por ende

sobre los activos "superiores"), refleja las consecuencias de las incidencias técnicas sobre el estado de los activos.

$$Riesgo = f(Impacto_{Activo}, Probabilidad_{Amenaza}) \tag{3.2}$$

El módulo de análisis de la plataforma de HSA consiste por tanto en la elaboración y actualización autónoma y en tiempo real, mediante la combinación de la información de incidentes no resueltos (RTIR) con la información de análisis de riesgos (PILAR) y de activos físicos (fuentes de datos físicos), de un grafo de dependencias del conjunto de activos del espacio híbrido, donde cada nodo de este alberga toda la información de estado actualizada del activo en cuestión (valor, criticidad, dependencias, amenazas sobre el mismo, incidentes que le afectan, niveles de riesgo, etc.).

Este procesamiento combinado de la información implica, por ende, no solo alcanzar un conocimiento pormenorizado y en tiempo real de la situación del espacio ciber-físico en su conjunto; sino también brindar mecanismos preventivos y proactivos de defensa, que suponen una notable mejora en el proceso de toma de decisiones, al permitir determinar las consecuencias que conllevaría la materialización de amenazas sobre el funcionamiento a futuro de la infraestructura crítica.

3.5.2. Análisis de inteligencia

En el caso de aplicar la arquitectura genérica de HSA propuesta a una solución de inteligencia híbrida, el análisis de datos hace referencia a todo análisis de inteligencia sobre datos de fuentes humanas, abiertas, de ámbito físico o ciber que proporcione información útil a los responsables de seguridad para el cumplimiento de su misión.

En esta línea, y como comentado anteriormente, se hacen necesarios métodos analíticos orientados a *Big Data* que, mediante el procesamiento de amplios conjuntos de datos y la extracción de características propias de estos, permitan determinar la evolución de los mismos y, por ende, predecir estados futuros. Estos datos, que pueden ser relativos tanto al mundo físico como al ciberespacio, pueden haber sido tanto recolectados por las fuentes de datos ciber (OSSIM, MISP o RTIR) o físicos como aportados por fuentes humanas.

En este contexto, se propone la integración en la plataforma de HSA de herramientas analíticas externas que implementan métodos de minería de datos [172] para, a través de procedimientos de análisis estadístico, detectar patrones relevantes y proporcionar conocimiento [274]. Las técnicas computacionales

empleadas por dichas herramientas consisten en algoritmos, supervisados (algoritmos de clasificación) o no supervisados (algoritmos de agrupamiento) [275], basados en aprendizaje automático [176] y ejecutados sobre los datos en bruto tanto estructurados como no estructurados.

Para la arquitectura aquí propuesta, y considerando las alternativas estudiadas en el capítulo 2, se opta inicialmente por la integración de la siguiente herramienta de análisis:

- **IBM i2 Analyst's Notebook**

  La solución analítica de IBM constituye la alternativa comercial por excelencia, de mayor prestigio y más extendida a nivel mundial en el ámbito del análisis de inteligencia. IBM i2 Analyst's Notebook [188] facilita al analista la comprensión de escenarios complejos combinando eficientes funcionalidades de análisis con potentes e intuitivas visualizaciones (redes conectadas, cronologías, vistas geoespaciales, etc.) para revelar conexiones, patrones y tendencias en amplios conjuntos de datos heterogéneos y de fuentes diversas. Además, dispone de un SDK propio principalmente compuesto de una extensa API que permite el acceso programático a gran parte de las capacidades de la herramienta.

Con todo, el diseño modular de la arquitectura presentada junto a una nueva capa de abstracción (*Analytic Tool Abstraction Layer* (ATAL)) que desacople, en este caso, el acceso a la herramienta de análisis del resto del sistema, facilitarían la inclusión a futuro de otras soluciones analíticas distintas.

En el caso por tanto de una solución de inteligencia híbrida, el módulo de análisis de la plataforma consiste en la ejecución, bien sea puntual o periódica, de análisis predefinidos sobre conjuntos de datos de diversas fuentes a través de la herramienta analítica integrada en el sistema (IBM i2 Analyst's Notebook) a tal fin y con el propósito de obtener la información de inteligencia requerida por el analista en cuestión.

3.6. Representación de información

Puesto que la arquitectura aquí definida se presenta como la de una herramienta eminentemente de visualización del espacio ciber-físico, es responsabilidad del módulo de representación de información el proveer la adecuada conciencia conjunta de la situación, o HSA, para mejorar la toma de decisiones en lo que a protección de infraestructuras críticas se refiere. Se trata por tanto de poder visualizar, de manera rápida e intuitiva, tanto el estado actualizado de

los activos como los resultados de todo tipo de análisis o consulta procesado en el módulo anterior. Así, por ejemplo, ante un evento como pueda ser la pérdida de comunicación con un determinado activo, se verá afectada la representación tanto de este como la de todos aquellos vinculados al mismo. De igual manera, la evaluación de consecuencias de un posible ataque a un activo en particular, influirá en el estado de todos aquellos que, a tenor de dicha simulación, se viesen afectados.

En esta línea, y de acuerdo tanto a las necesidades constatadas en el capítulo 2 como a los requisitos funcionales de ambos casos de uso, las capacidades de representación de información propuestas para el módulo de visualización son principalmente de tres tipos: visualizaciones georreferenciadas sobre GIS, visualizaciones avanzadas y visualizaciones inmersivas.

3.6.1. Información geolocalizada

La representación georreferenciada de la información, que constituye un elemento clave para adquirir una adecuada percepción del entorno, requiere, como es obvio, la utilización de al menos un sistema de información geográfica (GIS).

- **Luciad**

  Tanto por su actual posicionamiento en sectores estratégicos del mercado como por requerimientos de usuario, se ha optado finalmente por la integración de la herramienta LuciadLightspeed [209], de la compañía Luciad [208], como principal motor GIS de la plataforma de HSA propuesta. No en vano, gracias al sinfín de posibilidades que su extensa API ofrece para la representación en tiempo real, georreferenciada y multidimensional de información heterogénea, se sitúa hoy en día como la mejor opción para la generación de una COP del espacio ciber-físico en su conjunto.

- **Cesium**

  Adicionalmente, y con la finalidad de diversificar las tecnologías de representación geoespacial ofrecidas por la plataforma, se propone también la integración de Cesium [218] como herramienta GIS alternativa. En este caso, y como comentado anteriormente, se trata de un *framework* cartográfico de código abierto especialmente orientado a soluciones web. Avalada por su libre acceso y su amplia comunidad de soporte, las capacidades que hoy en día ofrece la biblioteca JavaScript de Cesium nada tienen que envidiar a las de algunas soluciones GIS comerciales.

De nuevo, la implementación de una capa de abstracción (*GIS Abstraction Layer* (GAL)) permitirá, en esta ocasión, no solo alternar de manera inmediata entre los dos motores GIS propuestos sino también simplificar la integración futura de otros nuevos.

Dependiendo de las capacidades específicas de cada herramienta geoespacial y del caso de aplicación de la arquitectura de HSA en cuestión, las funcionalidades generales que se proponen por tanto para el módulo de visualización en lo que a representación de información sobre GIS se refiere son las siguientes:

- Visualización geolocalizada y en tiempo real de activos físicos (personas, vehículos, instalaciones, etc.) y ciber (software, hardware, servicios, etc.).
- Representación de información conectada (dependencias entre activos, redes sociales, flujos de datos, etc.) mediante grafos tridimensionales georreferenciados.
- Codificación de información según estados por tamaño y/o color (objetos volumétricos) o densidad (mapas de calor).
- Utilización de iconos y simbologías estándar.
- Filtrado de la información representada (temporal, geográfico, por criticidad, etc.).
- Utilización de herramientas geométricas (inserción de objetos y polígonos, cálculo de distancias, perfil de terreno, etc.).
- Acceso a información de fuentes externas (fuentes abiertas, proveedores cartográficos, Google Places [276], etc.).
- Gestión individual de información visualizada por capas.

3.6.2. Diagramas y grafos

Como complemento a las capacidades de representación de información geolocalizada sobre GIS, se propone también la integración de métodos de visualización mediante grafos y diagramas [277][278]. Sin lugar a duda, estas constituyen una alternativa más que interesante para la ágil y rápida interpretación, mediante atractivas técnicas de representación, de conjuntos complejos de información relacional no necesariamente georreferenciables.

En este sentido, y de entre las herramientas existentes anteriormente revisadas, se opta finalmente por la integración en la plataforma tanto de la biblioteca Microsoft Chart Controls [225] para la generación de representaciones gráficas

convencionales en 2D o 3D, como del *framework* JavaScript Data-Driven Documents [230] para la producción de avanzados grafos y diagramas interactivos.

De manera sintética, la Tabla 3.3 recoge las principales representaciones gráficas seleccionadas por cada una de estas bibliotecas.

Clásicos	• *Point Chart* • *Bar Chart* • *Area Chart* • *Pie Chart* • *Funnel Chart*	• *Line Chart* • *Column Chart* • *Spline Area Chart* • *Radar Chart* • Etc.
Avanzados	• *Bubble Chart* • *Force-Directed Graph* • *Hebbian Dynamics* • *Code Flower* • *Collapsible Force Layout*	• *Circle Packing* • *Radial Dendogram* • *Zoomable Sun Burst* • *Zoomable Tree Map* • Etc.

Tabla 3.3: Principales grafos y diagramas.

3.6.3. Visualización inmersiva

Por último, y siempre que la aplicación de la arquitectura de HSA a cada caso de uso lo permita, se propone la integración adicional de capacidades de visualización inmersiva de la información. Como comentado en el capítulo 2, la interacción con mapas y grafos tridimensionales a través de técnicas de realidad virtual supone, sin lugar a duda, un considerable valor añadido para la adecuada percepción de la situación del entorno ciber-físico, sobre todo cuando la complejidad del mismo es tal que la observación tradicional en 2D puede resultar insuficiente.

A tal fin, y a tenor del análisis comparativo efectuado en el capítulo anterior, se sugiere la utilización de Oculus Rift [242], HMD de la compañía Oculus [252], como dispositivo VR del módulo de visualización de la plataforma de HSA. Por una parte, su compatibilidad tanto con Luciad como con las versiones más recientes de Cesium permitirá la visualización tridimensional e interactiva sobre cualquiera de los dos GIS de la presente arquitectura. Por otra parte, se propone también el uso de la plataforma Unity [253] para el diseño de avanzados entornos y grafos 3D con el fin de ofrecer una navegación útil e intuitiva entre complejas estructuras de información relacional.

Capítulo 4

Validación de la arquitectura: GESTPIC

4.1. Introducción

Enmarcada en el área de estudio de *Cyber Command & Control*, la herramienta GESTPIC (Gestión y Protección de Infraestructuras Críticas) constituye la solución de CySA desarrollada por el grupo de investigación de SATRD y destinada a la ágil y eficiente protección de infraestructuras críticas en el contexto híbrido actual.

En particular, GESTPIC supone la aplicación de la arquitectura genérica de HSA propuesta en la presente investigación a un novedoso sistema de seguridad ciber-física orientado a la defensa de toda clase de infraestructura crítica de ámbito civil. La solución supone un enfoque innovador en su ámbito al proporcionar, mediante técnicas avanzadas de representación, la COP conjunta de las dimensiones física y ciber en un espacio único de visualización que facilite la toma de decisiones al operador correspondiente.

Con el propósito de validar el modelo genérico de HSA planteado en esta tesis doctoral (capítulo 3) y como caso de uso principal de la presente investigación, este capítulo tiene por objetivo describir las necesidades conducentes al desarrollo de la herramienta GESTPIC así como detallar la arquitectura de la misma y los distintos módulos que la componen.

4.2. Motivación y objetivos

Ante la carencia de soluciones que, frente al nuevo paradigma de guerra híbrida, permitan conducir acciones de defensa en un espacio único para la toma de decisiones [279][280], el proyecto GESTPIC tuvo como principal objetivo el desarrollo de una herramienta que genere la COP conjunta de las dimensiones físicas y ciber como aplicación fundamental de C2 a la protección de infraestructuras críticas.

Con la finalidad de facilitar la toma de decisiones del responsable de seguridad, el carácter innovador de GESTPIC radica en el desarrollo de una herramienta de visualización dotada de las características tradicionales de un sistema clásico de percepción situacional o SA, esto es:

- Permitir al responsable de operaciones la adquisición, por integración de la CySA y de la PSA en un único "campo de batalla", de una consciencia conjunta de la situación de las dimensiones físicas y ciber (HSA).
- Poder proyectar la comprensión de la situación para predecir el curso futuro de las operaciones y favorecer con ello el proceso de toma de decisiones.

La HSA obtenida a través de la aplicación, que depende fundamentalmente del grado de detalle de la información representada, varía según el ámbito de toma de decisiones; distinguiéndose, en un principio, tres niveles diferentes:

- **Nivel estratégico**: enfocado a alto nivel, ofrece una vista general de los eventos e incidentes más relevantes, sin entrar al detalle de los diferentes sistemas y sus características.
- **Nivel operacional**: enfocado a nivel intermedio, muestra información de eventos, incidentes o nivel de riesgo de todos los activos.
- **Nivel técnico/táctico**: enfocado a bajo nivel, proporciona el máximo nivel de detalle de los activos (datos en bruto, *logs*, tráfico de red, etc.).

Además, como herramienta de visualización que es, GESTPIC implementa también avanzadas técnicas de visualización de la información, como aporte novedoso respecto a otras aplicaciones de percepción situacional, a través de:

- Representaciones tridimensionales.
- Grafos y diagramas avanzados.
- Visualizaciones inmersivas mediante VR.

4.2.1. Características principales

De acuerdo con las necesidades detectadas en materia de protección de infraestructuras críticas en el contexto híbrido actual, se definieron las siguientes como principales capacidades del sistema GESTPIC:

- Provisión de un sistema de monitorización que permita la generación y actualización en tiempo real de una HSA por integración de las situaciones en los dominios físicos (tierra, mar y aire) y en el ciberespacio.
- Representación geolocalizada, mediante una topología basada en grafos y en un único espacio de visualización, de las interrelaciones (enlaces) entre los diferentes activos (nodos) físicos y ciber.
- Visualización inmersiva, mediante capacidades de representación de VR, de la proyección sobre un mapa geográfico tridimensional de la topología de espacio único.
- Filtrado geográfico, temporal o por criticidad de la información representada en el mapa principal.
- Representación del estado de riesgo general de los activos (nodos) críticos para el correcto cumplimiento de las operaciones.
- Visualización, bajo demanda del operador, de información detallada sobre un activo crítico en sí, su nivel de riesgo o el estado de sus interrelaciones (enlaces) según un código normalizado.
- Representación, a modo de análisis de consecuencias, del estado de riesgo de los activos (nodos) físicos y ciber de producirse un determinado ataque.
- Estimación y actualización en tiempo real, en función de los eventos entrantes e incidentes en curso, del nivel de amenaza global sobre la red de activos.

4.2.2. Casos de uso

Una vez establecidos los requisitos de usuario de la aplicación, se determinaron los diferentes sistemas y actores de GESTPIC así como los diversos casos de uso de la solución.

Como muestra la Figura 4.1, los sistemas externos implicados en GESTPIC corresponden a las distintas fuentes de datos, tanto ciber como físicos, integradas en la herramienta:

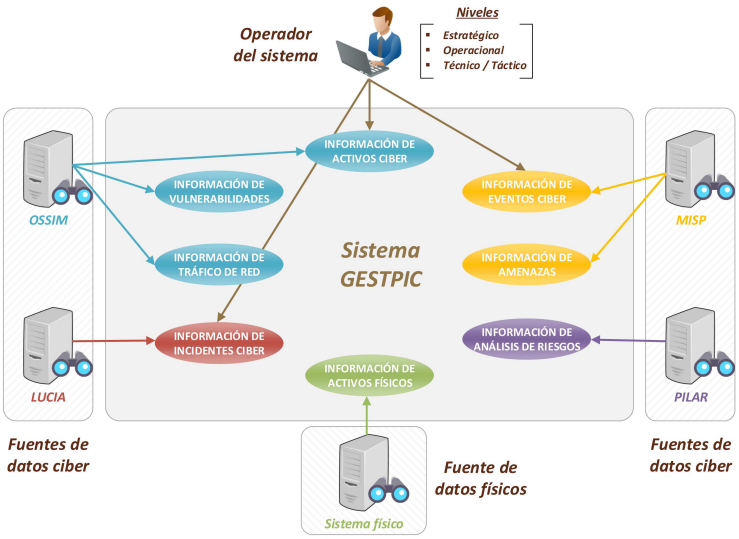


Figura 4.1: Sistemas y actores de GESTPIC.

- **OSSIM**: proporciona información sobre activos ciber (configuración, propiedades, servicios, etc.), vulnerabilidades y flujos de red.
- **MISP**: proporciona información sobre amenazas identificadas y sobre todo tipo de eventos ciber relevantes.
- **LUCIA**: versión adaptada de RTIR a las necesidades del CCN-CERT [167], proporciona información y seguimiento de ciberincidentes.
- **PILAR**: proporciona toda la información necesaria para el análisis de riesgos (valores, amenazas y riesgos de activos ciber).
- **Sistema físico**: proporciona toda la información relativa a activos físicos (personas, vehículos, instalaciones, etc.) y su localización en tiempo real.

Por su parte, los actores principales de la aplicación corresponden a los operadores de la misma. Estos se agrupan, como indicado anteriormente y dependiendo de sus necesidades de información y modo de interacción con el sistema, en tres categorías diferentes según su rol en la organización: nivel estratégico, nivel operacional y nivel técnico/táctico.

Si bien el flujo de información con los sistemas externos es mayoritariamente unidireccional (de las fuentes de datos a GESTPIC), el operador del sistema (independientemente de su rol) está habilitado tanto para consumir la información proporcionada por estos como para la inserción manual de toda aquella relativa a activos, eventos o incidentes.

La Tabla 4.1 presenta los diferentes casos de uso definidos para el sistema GESTPIC clasificados en seis categorías básicas: (i) obtención de información, (ii) inserción manual, (iii) análisis, (iv) visualización de información, (v) generación de SA y (vi) exportación de información.

Categoría	**Descripción**
Obtención de información	• Obtención de información de activos ciber de OSSIM. • Obtención de información de alarmas de OSSIM. • Obtención de información de vulnerab. de OSSIM. • Obtención de información de eventos de MISP. • Obtención de información de amenazas de MISP. • Obtención de información de incidentes de LUCIA. • Obtención de información de riesgos de PILAR. • Obtención de información de activos físicos.
Inserción manual	• Inserción manual de activos ciber. • Inserción manual de amenazas. • Inserción manual de incidentes.
Análisis	• Fusión de información obtenida de las diversas fuentes siguiendo un modelo de datos propio y almacenamiento en base de datos. Generación de COP personalizada a los diversos roles y necesidades.
Visualización de información	• Visualización de información global o filtrado por una determinada dimensión/variable. • Visualización de información detallada de activos ciber y físicos. • Visualización de información relativa a alarmas y los activos a los que estén asociadas. • Visualización de información relativa a vulnerabilidades y los activos a los que estén asociadas. • Visualización de información relativa a eventos y los activos a los que están asociados. • Visualización de información relativa a incidentes y los activos a los que están asociados.

Generación de SA	• Generación de la SA ciber (CySA) a partir de información anteriormente obtenida. • Generación de la SA física (PSA) a partir de información anteriormente obtenida. • Generación de la SA híbrida (HSA) a partir de información anteriormente obtenida. • Generación de la SA híbrida (HSA) para su visualización inmersiva en dispositivos de VR. • Conmutación de la COP entre las tres vistas principales (estratégica, operacional y táctica).
Exportación de información	• Exportación a fichero, siguiendo el modelo de datos propio, de información del sistema.

Tabla 4.1: Casos de uso de GESTPIC.

4.3. Arquitectura del sistema

La Figura 4.2 describe la arquitectura del sistema aquí presentado y sus principales componentes. Diseñada de manera modular con el fin de proporcionar escalabilidad y desacoplar el funcionamiento de los distintos componentes, esta se constituye a partir de una serie de módulos funcionales implementados de manera independiente:

- **Núcleo del sistema**: módulo principal de la aplicación (o *kernel* del sistema) responsable de las tareas nucleares de la herramienta y de la interconexión del resto de sus módulos. Gestiona y supervisa, además, el correcto funcionamiento de todos estos.
- **Módulo de interoperabilidad**: responsable de la comunicación con los sistemas externos de la aplicación y de la adquisición de información ciber y física desde estos.
- **Módulo de acceso a BBDD**: coordina el acceso y las peticiones de información a la base de datos de la herramienta.
- **Módulo de análisis y correlación**: encargado de las funcionalidades analíticas del sistema como el estado de activos, análisis de riesgos, nivel de amenaza, etc.
- **Módulo de GIS**: administra el funcionamiento y la interacción con los distintos sistemas de GIS integrados en la aplicación.

- **Módulo de generación de visualizaciones**: responsable de la producción de todo tipo de representaciones de la información para su visualización en GIS o mediante grafos y diagramas.

- **Módulo de visualización inmersiva**: gestiona la generación de representaciones 3D de la información para su visualización inmersiva mediante VR.

- **Módulo HMI**: constituye la interfaz de usuario del sistema a través de la cual se reciben las peticiones del operador correspondiente.

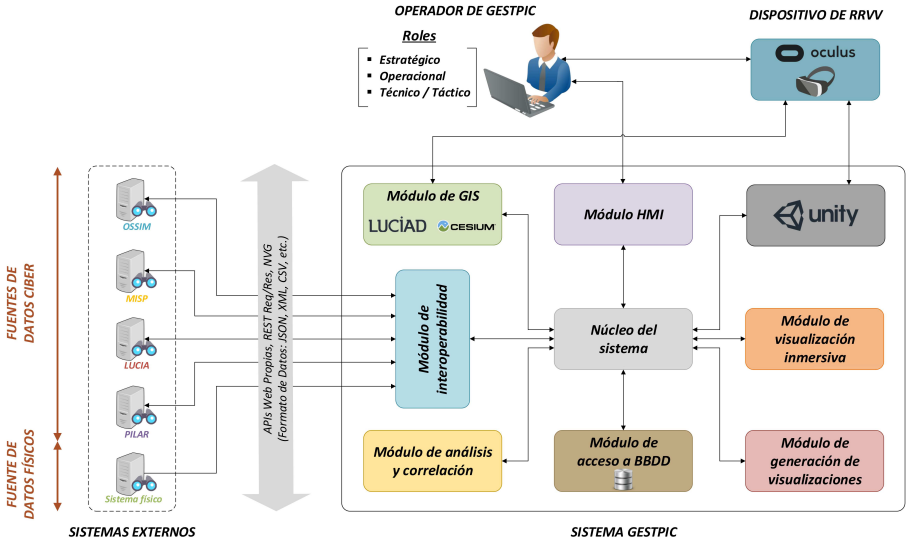


Figura 4.2: Arquitectura del sistema.

Como queda reflejado, la aplicación fusiona, a partir de un modelo de datos propio que constituye el eje principal de la misma, la información ciber y física previamente recogida de fuentes externas de datos (OSSIM, MISP, LUCIA, PILAR y sistema físico) y almacenada en la base de datos de la herramienta. De dicha combinación de la información deriva la obtención, mediante completas capacidades analíticas y técnicas avanzadas de representación, de una consciencia situacional del entorno ciber-físico en un espacio único de visualización para la toma de decisiones por parte del operador del sistema.

La solución es una aplicación ejecutable escrita en lenguaje C# y desarrollada en entorno .NET [281] que, definida de manera desacoplada y flexible, está pensada tanto para cumplir con las diferentes necesidades según el usuario en cuestión como para facilitar la adaptación de la misma a futuros nuevos requerimientos.

La presente arquitectura constituye por consiguiente una implementación, en sistema de defensa y seguridad ciber-física, del modelo genérico de HSA propuesto en el capítulo 3 para su aplicación a la adecuada protección de todo tipo de infraestructura crítica en el contexto híbrido actual.

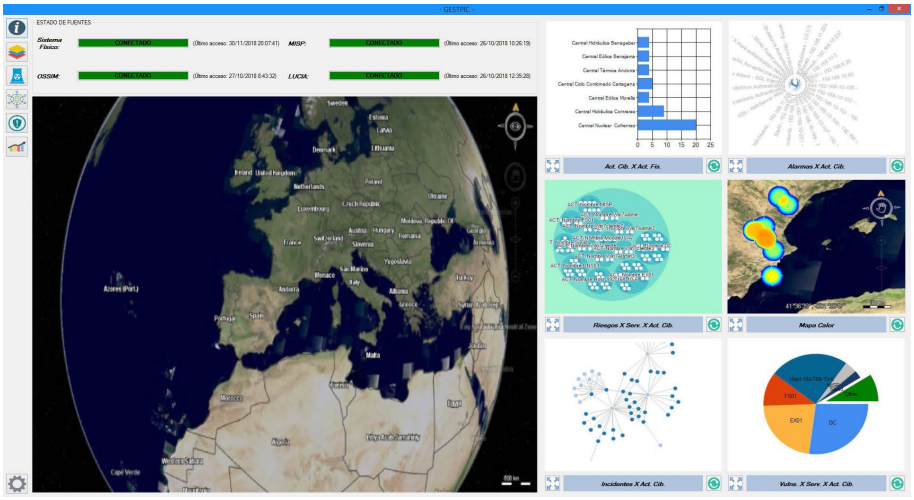


Figura 4.3: Vista principal de GESTPIC.

La Figura 4.3, que muestra la vista principal del sistema GESTPIC, revela de manera inmediata el protagonismo que, como herramienta eminentemente de visualización que es, tienen en ella los elementos de representación de la información.

En particular y como elemento más destacado, aparece el mapa principal de la herramienta. Independientemente del GIS (Luciad o Cesium) en uso, este permite navegar por una visualización 2D/3D de una cartografía del mundo en la que se representan, de manera georreferenciada, los activos físicos y sus activos ciber asociados. A la derecha del mismo se distribuyen hasta un total de seis paneles gráficos totalmente configurables para la representación de cualquier tipo de información bien sea, de nuevo, de manera geolocalizada sobre mapa o bien sea mediante múltiples tipos de grafos y diagramas disponibles.

En la parte superior, se muestra el estado actual de disponibilidad de los distintos sistemas externos así como la fecha y hora de la última comunicación con cada uno de ellos. Por último, una serie de botones ubicados verticalmente en la parte izquierda de la ventana constituyen el menú principal del sistema y permiten al usuario de GESTPIC acceder a las diversas funcionalidades que ofrece la herramienta.

4.3.1. Módulo de interoperabilidad

El módulo de interoperabilidad (Figura 4.4) es responsable de adquirir toda la información relativa a las dimensiones físicas y ciber de las fuentes externas de datos para su combinación y almacenamiento en la base de datos del sistema.

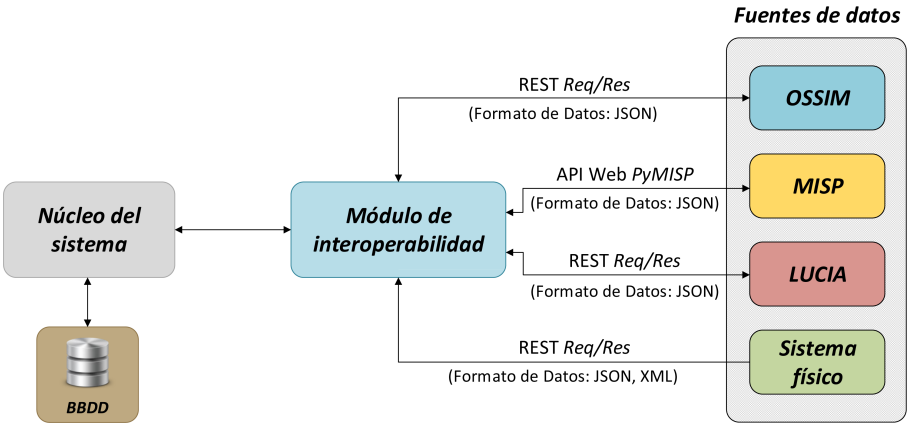


Figura 4.4: Módulo de interoperabilidad.

Como comentado en el capítulo 3 y como ilustra la Figura 4.5, la comunicación con dichas fuentes de datos se lleva a cabo a través bien de sus APIs web específicas (AlienVault API [258], PyMISP [260], RT API REST2 [261]), de llamadas REST estándar a través del mecanismo de Petición-Respuesta o incluso mediante protocolo NVG; y siempre mediante el intercambio de datos en formatos estándar (JSON, XML, etc.).

Este módulo puede ser configurado, bajo decisión del operador del sistema, para operar de manera ya sea periódica o bajo petición del usuario en lo que a la recolección de información se refiere.

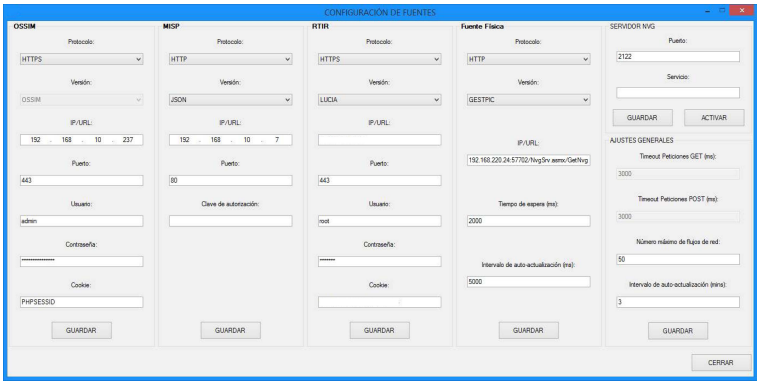


Figura 4.5: Configuración de fuentes externas.

4.3.2. Módulo de acceso a BBDD

El módulo de acceso a base de datos (Figura 4.6) es responsable de gestionar las consultas a la base de datos de GESTPIC, donde queda almacenada y relacionada, siguiendo un modelo de datos propio, toda la información adquirida de los sistemas externos (fuentes de datos ciber y físicos) de la herramienta.

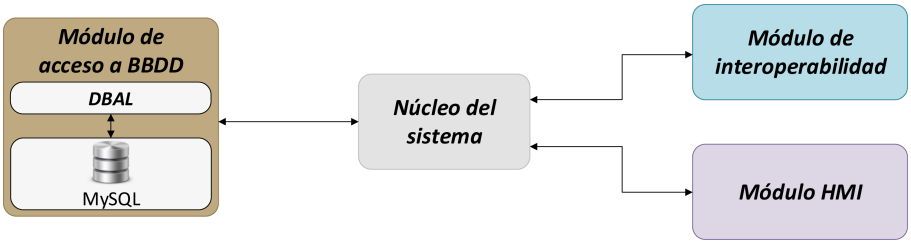


Figura 4.6: Módulo de acceso a BBDD.

Este módulo recibe peticiones tanto del módulo de interoperabilidad (para la actualización de la información adquirida de fuentes externas) como del módulo HMI (para la ampliación y refresco de las representaciones en curso, la generación de nuevas visualizaciones o la inserción manual de información por parte del usuario).

Pese a que, como comentado anteriormente, MySQL es la base de datos inicialmente desplegada en el sistema GESTPIC, la implementación del presente módulo a modo de capa de abstracción (*Database Abstraction Layer* (DBAL))

facilitaría la adaptación de la herramienta a bases de datos distintas en el futuro.

4.3.3. Módulo de análisis y correlación

El módulo de análisis y correlación de datos (Figura 4.7) es responsable de resolver, mediante mecanismos simples de procesado y análisis de los datos almacenados en la base de datos de GESTPIC, toda consulta analítica efectuada por el operador del sistema a través del módulo HMI.

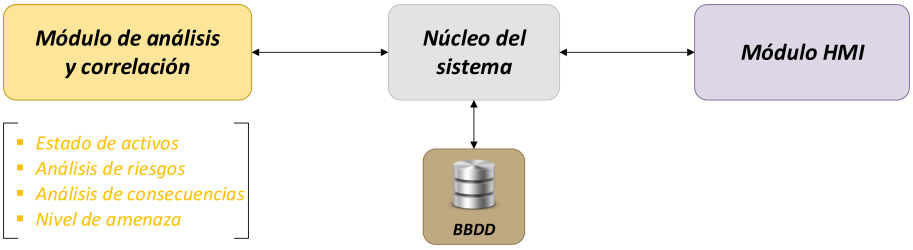


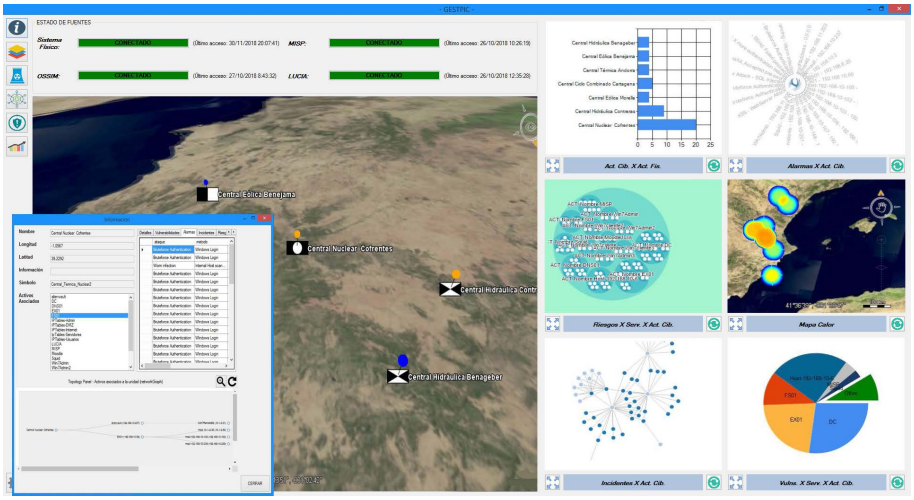
Figura 4.7: Módulo de análisis y correlación.

Partiendo siempre de la metodología MAGERIT, las peticiones que el presente módulo atiende son fundamentalmente cuatro: (i) el estado de activos físicos (Figura 4.8(a)) y ciber (Figura 4.8(b)), (ii) el nivel de amenaza global, (iii) el análisis de riesgos sobre el conjunto de activos (Figura 4.9(a)) y (iv) la evaluación de consecuencias ante un determinado ataque (simple o combinado) en particular (Figura 4.9(b)).

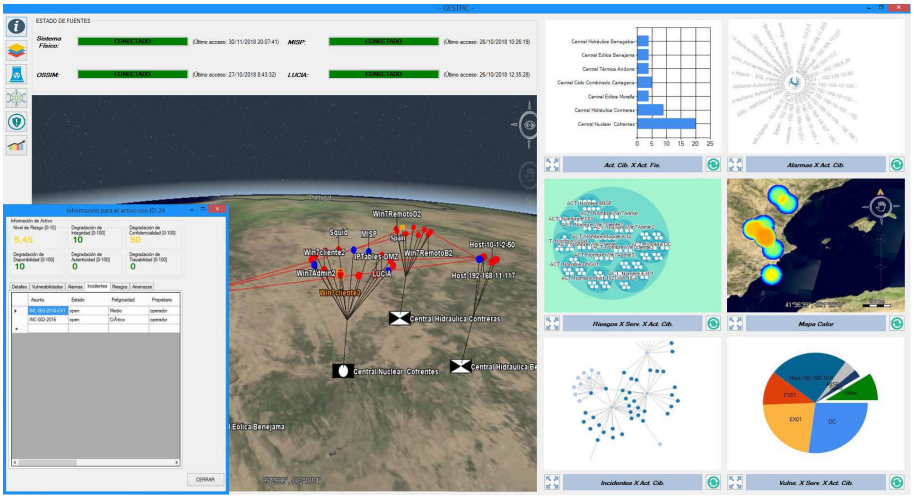
En lo que al riesgo de los activos ciber se refiere, se obtienen las amenazas asociadas a todos los incidentes activos que afectan a cada uno de estos y se devuelve, como valor actual de riesgo de cada activo ciber, el mayor de los riesgos acumulados de entre los correspondientes a todas sus amenazas.

De igual manera, el valor de riesgo de los activos físicos corresponde al mayor de los riesgos de los activos ciber asociados a cada uno de ellos.

Por nivel de amenaza se entiende, sin embargo, un valor porcentual del riesgo acumulado del conjunto de activos ciber respecto al riesgo máximo alcanzable en caso de materializarse la totalidad de las amenazas que se ciñen sobre todos ellos, y donde el riesgo de cada uno de estos viene ponderado por la criticidad del mismo.

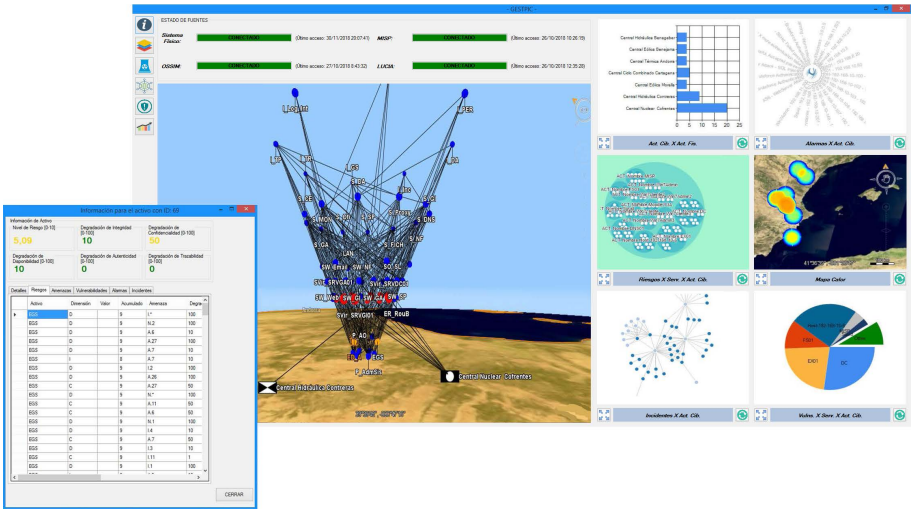


(a) Estado de activos físicos

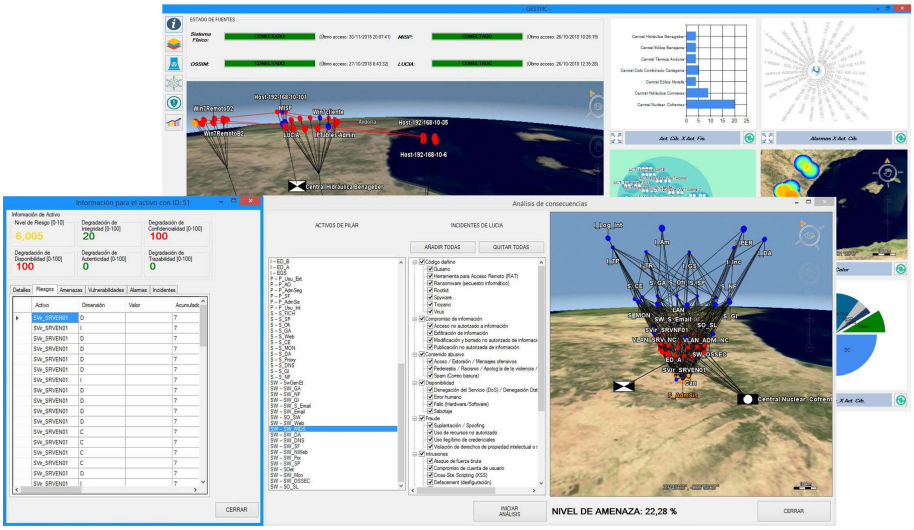


(b) Estado de activos ciber

Figura 4.8: Estado de activos físicos y ciber.



(a) Análisis de riesgos



(b) Análisis de consecuencias

Figura 4.9: Análisis de riesgos y de consecuencias.

4.3.4. Módulo de GIS

El módulo de GIS (Figura 4.10) es responsable de gobernar los sistemas de información geográfica (GIS) existentes en GESTPIC. En particular, gestiona en todo momento la interacción del operador del sistema, a través del módulo HMI, con la herramienta GIS en uso (navegación por el mapa, selección de elementos, cliqueo de objetos, etc.).

Tal y como comentado en el capítulo 3, los sistemas GIS inicialmente integrados en GESTPIC son Luciad y Cesium. Mediante la implementación de una capa de abstracción (*GIS Abstraction Layer* (GAL)), el presente módulo desacopla el núcleo del sistema del funcionamiento propio de cada herramienta cartográfica, permitiendo así la rápida y sencilla conmutación entre estas.

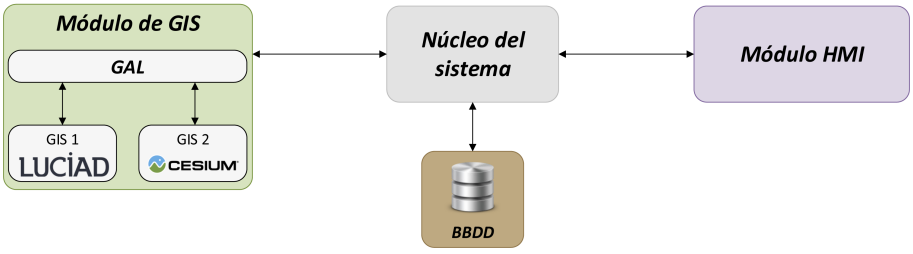


Figura 4.10: Módulo de GIS.

4.3.5. Módulo de generación de visualizaciones

El módulo de generación de visualizaciones (Figura 4.11) es responsable de atender, a través del módulo HMI, las peticiones del operador del sistema relativas a la representación de información almacenada en la base de datos de GESTPIC.

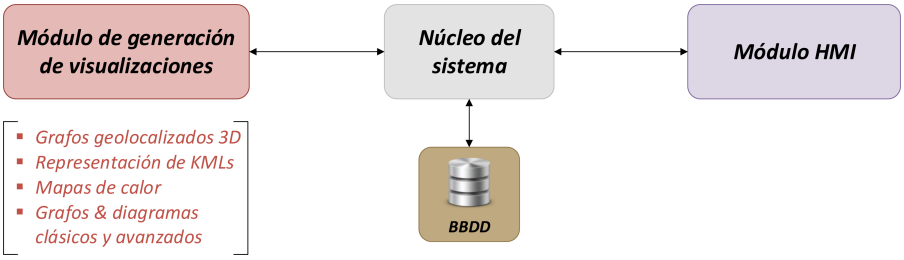


Figura 4.11: Módulo de generación de visualizaciones.

Dichas peticiones abarcan tanto las capacidades analíticas del sistema (estado de activos, análisis de riesgos o análisis de consecuencias) como cualquier tipo de combinación de información destinada a su visualización geolocalizada sobre el GIS en uso o mediante grafos y diagramas.

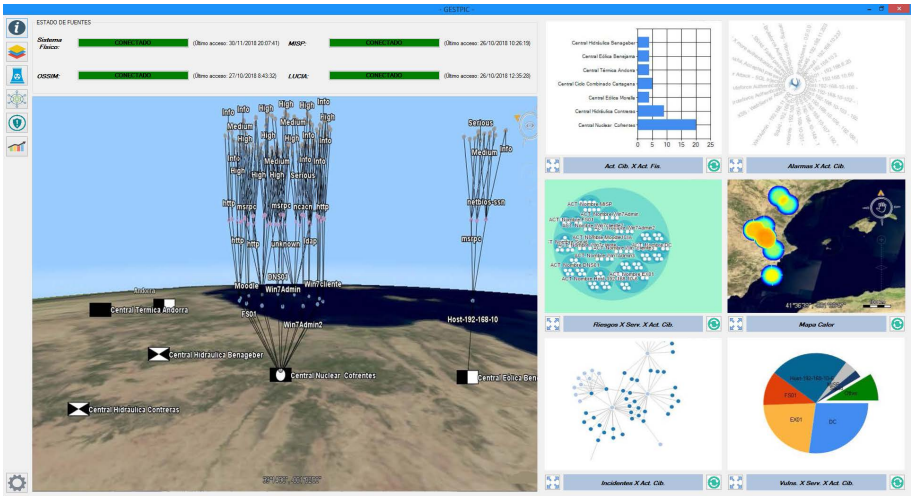
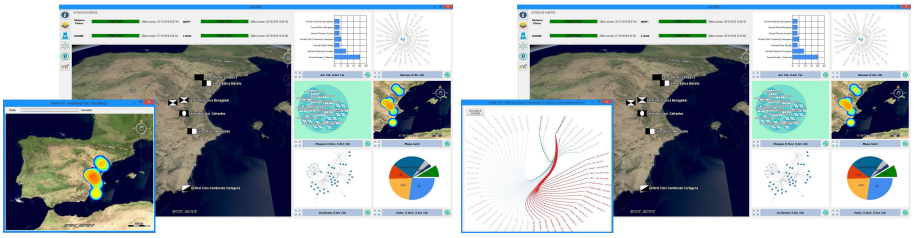


Figura 4.12: Grafos 3D georreferenciados.

La generación de grafos georreferenciados tridimensionales constituye la principal y más interesante técnica de representación de información sobre GIS (Figura 4.12). Adicionalmente, el sistema permite también la representación de datos espaciales en formato *Keyhole Markup Language* (KML) [282] o de mapas de calor (Figura 4.13(a)).



(a) Mapas de calor (b) Diagramas avanzados

Figura 4.13: Otras representaciones.

Además, en la medida de lo posible, se hace uso tanto de iconos como de simbologías estándar y, con el fin de resaltar estados y anomalías, se emplea codificación normalizada de la información por color y volumen.

En lo que a visualizaciones mediante grafos y diagramas se refiere (Figura 4.13(b)), estas comprenden, como comentado en el capítulo 3, desde *charts* convencionales (*point chart*, *area chart*, *column chart*, etc.) hasta avanzadas representaciones (*circle packing*, *force-directed graph*, *dendogram*, etc.).

4.3.6. Módulo de visualización inmersiva

El módulo de visualización inmersiva (Figura 4.14) es responsable de administrar la representación de información tanto ciber, como física o híbrida para su visualización en entorno inmersivo a través del dispositivo de VR.

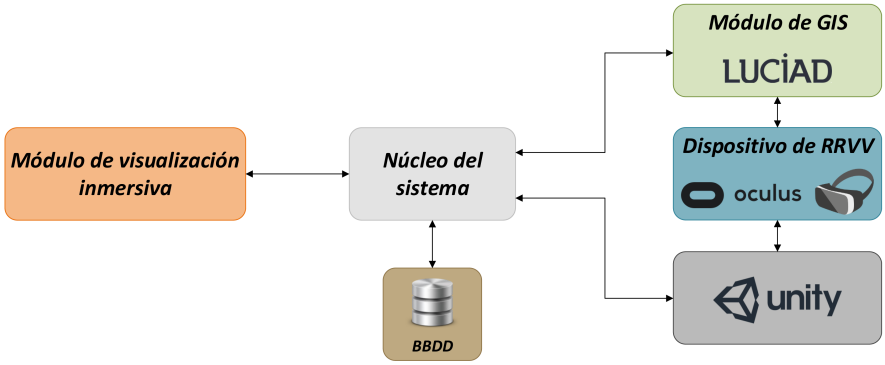
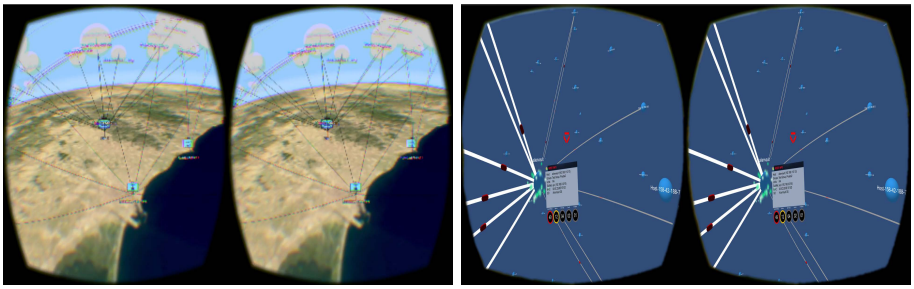


Figura 4.14: Módulo de visualización inmersiva.

Mediante este último, es posible navegar e interactuar en un espacio tridimensional tanto con el GIS y sus grafos geolocalizados 3D (Figura 4.15(a)) como entre complejas redes de información ciberreferenciada (Figura 4.15(b)).

Tal y como indicado previamente, el dispositivo VR inicialmente integrado en GESTPIC es el HMD Oculus Rift. La plataforma Unity es, por su parte, responsable del diseño del entorno tridimensional para la representación 3D de estructuras de información relacional.



(a) VR sobre GIS (Oculus & Luciad) (b) VR en ciberespacio (Oculus & Unity)

Figura 4.15: Visualización inmersiva.

4.3.7. Módulo HMI

El módulo HMI (Figura 4.16) constituye la interfaz del sistema GESTPIC con el usuario del mismo. Este es por tanto responsable de transmitir al núcleo del sistema los *inputs* recibidos por parte del operador con el fin de acometer la tarea solicitada.

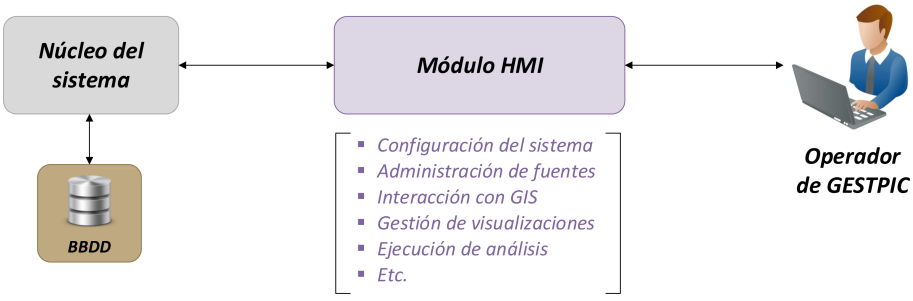


Figura 4.16: Módulo HMI.

Desde el presente módulo, el operador de GESTPIC puede, entre otros, interactuar con los componentes de visualización de información (GIS, grafos y diagramas), gestionar las diversas representaciones en curso, ejecutar funcionalidades de análisis (análisis de riesgos, análisis de consecuencias, nivel de amenaza, etc.) o administrar la configuración tanto de las fuentes externas de datos como del sistema en sí.

Capítulo 5

Evaluación del sistema GESTPIC

5.1. Introducción

El grupo de investigación de SATRD inicia en 2014, como comentado en anteriores capítulos, una nueva sub-línea de investigación denominada *Cyber Command & Control* cuya principal finalidad es la aplicación de los conocimientos adquiridos en el desarrollo de sistemas de información para mando y control (C4ISR) a los ámbitos de la ciberdefensa y la ciberseguridad. En esta línea, la presente investigación propone una arquitectura orientada a la adecuada protección de infraestructuras críticas en el entorno ciber-físico que, por integración de la CySA a la SA tradicional, permita la visualización de la COP conjunta en un espacio único para la toma de decisiones.

El presente capítulo tiene por tanto como objetivo, una vez validado el modelo propuesto en esta investigación a través de la implementación del sistema GESTPIC (capítulo 4), la evaluación de este último como caso de uso principal de la presente tesis doctoral.

Para ello, se detallarán los requisitos y especificaciones técnicas de la solución, se presentará el escenario empleado para la completa evaluación, tanto técnica como operativa, del sistema y se describirá el conjunto de pruebas efectuado a tal fin. Por último y de manera adicional, se expondrá la actual participación de GESTPIC en el proyecto europeo SAURON como uno de los contextos de uso más relevantes de la aplicación.

5.2. Evaluación de GESTPIC

Con motivo de la finalización del proyecto GESTPIC, se llevó a cabo una exhaustiva evaluación de prestaciones de un prototipo de la solución desarrollada con el fin de probar su correcto funcionamiento y el cumplimiento de los requerimientos inicialmente establecidos.

Para ello, tras revisar las especificaciones técnicas y los requisitos mínimos necesarios para la utilización del demostrador implementado, se describe el escenario de pruebas propuesto para la completa evaluación, tanto técnica como operativa, del sistema GESTPIC y, posteriormente, se presenta el conjunto de tests funcionales llevados a cabo.

5.2.1. Especificaciones técnicas

El correcto funcionamiento de la herramienta GESTPIC precisa tanto de un entorno mínimo de hardware adecuado a las especificaciones de los diferentes sistemas involucrados (con el soporte para visualización inmersiva mediante VR como mayor restricción) así como de un conjunto de software previo requerido por los distintos componentes que integran la solución (base de datos, sistemas GIS, motores gráficos, *frameworks* y bibliotecas, etc.).

Así pues, seleccionado en la fase de definición del proyecto como dispositivo VR para la visualización de información en entorno inmersivo y como requerimiento hardware más exigente del sistema GESTPIC, la Tabla 5.1 presenta, de manera sintética, las principales especificaciones técnicas de Oculus Rift [242].

Pantalla	OLED
Resolución	2160 x 1200
Tasa de refresco	90 Hz
Campo de visión	110 º
Sensores	Acelerómetro, magnetómetro, giroscopio, cámara de *tracking*

Tabla 5.1: Especificaciones técnicas de Oculus Rift [1].

[1] Oculus Rift, `https://www.oculus.com/rift` [Accessed Apr. 26, 2018].

Además, la utilización de un dispositivo de estas características implica el uso de una tarjeta gráfica, a poder ser dedicada, de alto rendimiento.

Núcleos CUDA	1664
Frecuencia de reloj normal / acelerada	1050 MHz / 1178 MHz
Memoria	4 GB
Ancho de banda de memoria	224 GB/s
Máxima resolución digital / VGA	5120 x 3200 / 2048 x 1536

Tabla 5.2: Especificaciones técnicas de NVIDIA GeForce GTX 970 [2].

En concreto, se optó por NVIDIA GeForce GTX 970 [283], de entre las alternativas disponibles en la fase de diseño del sistema, como tarjeta gráfica con especificaciones técnicas (Tabla 5.2) mínimamente compatibles con Oculus Rift.

De este modo, pudieron determinarse las necesidades mínimas de hardware para el normal y completo funcionamiento de la solución GESTPIC, las cuales vienen recogida de manera resumida en la Tabla 5.3.

Procesador	Intel Core i7 de 64 bits
Disco Duro	HDD de 1 TB
Memoria	12 GB de RAM
Tarjeta gráfica	NVIDIA GeForce GTX 970

Tabla 5.3: Requisitos mínimos de hardware.

En caso de querer prescindir de soporte para visualización inmersiva mediante VR, los requisitos mínimos de hardware que necesitaría el sistema GESTPIC para operar adecuadamente serían, como puede verse en la Tabla 5.4, sin lugar a duda menos restrictivos.

[2] NVIDIA GeForce GTX 970, `https://www.geforce.com/hardware/desktop-gpus/geforce-gtx-970` [Accessed Nov. 29, 2018].

Procesador	Intel Core i5 de 64 bits
Disco Duro	HDD de 1 TB
Memoria	8 GB de RAM
Tarjeta gráfica	Intel HD Graphics 4600

Tabla 5.4: Requisitos mínimos de hardware sin VR.

En lo que a requerimientos de software se refiere, el adecuado funcionamiento del sistema GESTPIC precisa de la previa instalación del siguiente software externo:

- Windows 8/8.1/10 de 64 bits.
- Microsoft .NET Framework 3.5 y 4.5.2.
- Microsoft Visual C++ Redistributable 2013.
- MySQL Server 5.5.54 y Connector .NET 6.9.5.
- Microsoft *Internet Information Services* (IIS) Express 10.0.
- Java SE Development Kit 8.
- Oculus SDK Runtime 0.8.0.0 (opcional).

5.2.2. Escenario de pruebas

Con el fin de llevar a término las distintas pruebas de evaluación del sistema GESTPIC, fue necesaria la previa definición de un escenario apropiado a tal fin. Este consistió, inicialmente, en la implementación de un muy completo y realista entorno virtualizado de red [284] desplegado mediante el software VMware vSphere ESXi [285] como hipervisor de la plataforma y VMWare vCenter Server [286] como servidor principal para la gestión centralizada y automatizada de la infraestructura virtual al completo.

Como puede verse de manera muy esquemática en la topología de red de la Figura 5.1, dicho entorno virtual (área gris) se compone principalmente de, por un lado, una subred en la que, además del sistema GESTPIC, se hallan los diferentes sistemas externos que ejercen de fuentes de datos del mismo (OSSIM,

MISP, LUCIA, etc.) así como una serie de servidores adicionales (servidores *SharePoint*, FTP, de correo, etc.); y, por otro lado, una subred independiente (*De-Militarized Zone* (DMZ)) que alberga servicios habituales en servidores expuestos (servidores *proxy*, DNS, web, etc.). El entorno virtual, que también es accesible por usuarios externos y nodos remotos, se completa con equipos para usuarios internos y administradores.

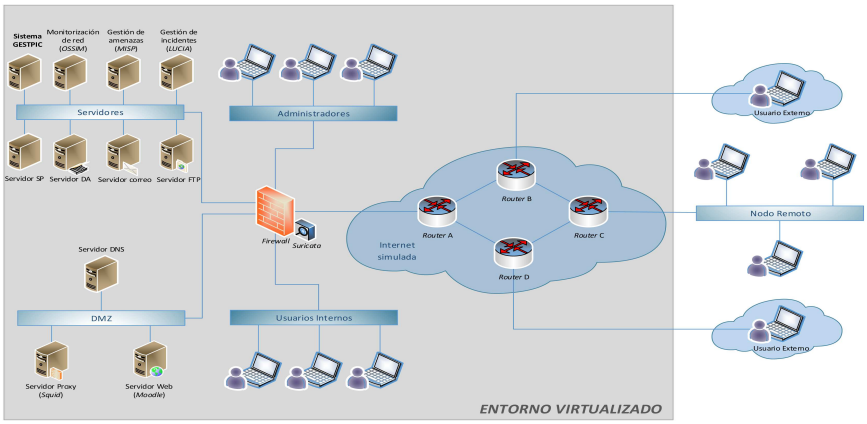


Figura 5.1: Entorno virtualizado de pruebas.

En un primer momento, se partió de un escenario básico en el que, sin acceso a sistemas externos, se pudo comprobar las prestaciones de la herramienta GESTPIC haciendo únicamente uso de información, almacenada en base de datos, previamente adquirida de sus fuentes de datos físicos y ciber.

Posteriormente, se llevó a cabo la evaluación completa de la aplicación en la que, esta vez sí, el sistema GESTPIC adquiría y actualizaba en tiempo real la información ciber-física que obtenía de las distintas fuentes de datos conectadas al mismo.

Por último, una vez probado el sistema en un entorno más bien controlado como el aquí simulado, se repitió el mismo conjunto de pruebas al completo pero, en esta ocasión, en un entorno de uso real desplegado específicamente a tal fin y muy similar al aquí descrito.

5.2.3. Evaluación de la solución

A continuación se listan, de manera resumida, el conjunto de pruebas llevadas a cabo en los escenarios anteriormente descritos para la evaluación, tanto técnica como operativa, del sistema GESTPIC.

Por una parte, la evaluación técnica del sistema consistió en un conjunto de pruebas atómicas y muy específicas destinadas a comprobar, de manera individual, el independiente y correcto funcionamiento de las distintas características y funcionalidades que ofrece el sistema.

En concreto y como muestra la Tabla 5.5, esta batería de pruebas abarcó desde pruebas de configuración de los distintos sistemas externos hasta diversas pruebas de visualización pasando por multitud de pruebas de gestión tanto de la información almacenada como de las capacidades de representación de la misma.

Categorías	**Pruebas de evaluación**
Software	• Prueba de funcionamiento en Window 8.1 • Prueba de funcionamiento en Window 10 • Prueba de instalación del sistema
Configuración	• Prueba de configuración de OSSIM • Prueba de configuración de MISP • Prueba de configuración de LUCIA • Prueba de configuración general
Asociación	• Prueba de asociación de eventos • Prueba de asociación de incidentes • Prueba de asociación de activos físicos • Prueba de asociación de operaciones • Prueba de asociación de información de AARR
Gestión de entidades	• Prueba de modificación de activos físicos • Prueba de modificación de activos ciber • Prueba de modificación de operaciones • Prueba de modificación de información de AARR
Obtención de datos	• Prueba de obtención automática de datos • Prueba de obtención manual de datos • Prueba de obtención de datos físicos • Prueba de programación de escaneos de red
Gestión de BBDD	• Prueba de importación de fichero de datos • Prueba de exportación de fichero de datos • Prueba de borrado de base de datos
Gestión de representación	• Prueba de creación de consultas a base de datos • Prueba de salvado de consultas a base de datos • Prueba de carga de consultas a base de datos • Prueba de borrado de consultas a base de datos

GIS	• Prueba de visualización de activos físicos • Prueba de visualización de nombre de activos físicos • Prueba de visualización de información física • Prueba de visualización de información ciber
Visualización	• Prueba de visualización de diagramas clásicos • Prueba de visualización de diagramas avanzados • Prueba de visualización de grafos 3D geolocalizados • Prueba de visualización de datos en formato KML • Prueba de visualización de mapas de calor • Prueba de visualización de gestor de capas • Prueba de recarga de información actualizada
Visualización inmersiva	• Prueba de visualización en entorno inmersivo de VR • Prueba de navegación en entorno inmersivo de VR

Tabla 5.5: Pruebas de evaluación técnica del sistema.

Por otra parte, la evaluación operativa del sistema se basó en otra serie de pruebas, en este caso mucho más complejas y secuenciales, orientadas a valorar el cumplimiento de los requisitos operativos del sistema y el grado de utilidad de la misma en entornos reales de uso.

En concreto y como muestra la Tabla 5.6, este conjunto de pruebas permitió probar, entre otras, las distintas capacidades analíticas de la herramienta, la representación destacada de estados anómalos, la generación de la adecuada HSA o la visualización de información ciber-física en un único espacio de representación.

Categorías	**Pruebas de evaluación**
Generación de HSA	• Prueba de visualización de HSA mediante generación de diagramas avanzados • Prueba de visualización de HSA mediante "Estado de activos" físicos y ciber
Espacio ciber-físico	• Prueba de visualización de dominios físico y ciber en espacio único mediante generación de grafos georreferenciados 3D • Prueba de visualización de relaciones entre información ciber y física mediante generación de grafos georreferenciados 3D

Capacidades de análisis	• Prueba de visualización de información detallada de riesgos mediante "Análisis de riesgos" • Prueba de visualización de información detallada de riesgos mediante "Gestión de datos PILAR" • Prueba de visualización de riesgo global del entorno mediante "Nivel de amenaza" • Prueba de simulación de ataques mediante "Análisis de consecuencias"
Filtrado de información	• Prueba de filtrado temporal mediante generación de consultas a BBDD • Prueba de filtrado por operaciones mediante generación de consultas a BBDD • Prueba de filtrado por activos mediante generación de consultas a BBDD • Prueba de filtrado por criticidad de activos mediante generación de consultas a BBDD
Áreas de interés	• Prueba de visualización de mapa principal en sub-áreas geográficas mediante interacción con GIS • Prueba de visualización de mapa principal en sub-áreas geográficas mediante representaciones georreferenciadas en paneles gráficos • Prueba de visualización de mapa principal en sub-áreas geográficas mediante aplicación de filtro geográfico
Flexibilidad de representación	• Prueba de conmutación entre representaciones geogerefenciadas y grafos/diagramas • Prueba de conmutación entre representaciones geogerefenciadas y entorno inmersivo de VR • Prueba de conmutación entre distintos tipos de grafos y diagramas clásicos/avanzados
Estados anómalos	• Prueba de visualización destacada de activos afectados por alarmas ciber • Prueba de visualización destacada de activos afectados por incidentes ciber

Tabla 5.6: Pruebas de evaluación operativa del sistema.

Los resultados obtenidos de la ejecución de estas pruebas de evaluación en los distintos escenarios anteriormente presentados fueron del todo satisfactorios, no constatándose deficiencia funcional u operativa alguna.

5.3. Participación en proyecto SAURON

En la actualidad y hasta abril de 2020, el grupo de investigación de SATRD participa, entre otros, en el proyecto europeo SAURON [84][287], correspondiente al programa de investigación e innovación H2020 de la Comisión Europea [85]. SAURON está enfocado al desarrollo de soluciones de mando y control orientadas a la protección de infraestructuras críticas de ámbito portuario, y en él participan:

- **Operadores portuarios (usuarios finales)**: *Fundación Valencia Port* (España) (coordinador) [288], *Noatum* (España) [289], *Autoridad Portuaria del Pireo* (Grecia) [290], *Autoridad Portuaria de Livorno* (Italia) [291] y *Puerto de Koper* (Eslovenia) [292].

- **Universidades y centros de investigación**: *Universidad Politécnica de Valencia* (España) [293], *Universidad del Pireo* (Grecia) [294], *Universidad Católica de Lovaina* (Bélgica) [295] y *Austrian Institute of Technology* (Austria) [296].

- **Empresas tecnológicas**: *Thales* (Francia) [297], *Morpho* (Francia) [298], *Grupo ETRA* (España) [299], *S2 Grupo* (España) [300] e *InnovaSec* (Ucrania) [301].

El principal objetivo de SAURON [302] es el de proporcionar una plataforma multidimensional de SA que permita a operadores y autoridades portuarias anticiparse y responder adecuadamente frente a potenciales amenazas, tanto físicas como ciber o combinadas, a la seguridad de sus instalaciones portuarias como a la de trabajadores, pasajeros y ciudadanos presentes en las inmediaciones (Figura 5.2). Más concretamente, el proyecto propone un concepto holístico de SA como solución integral, escalable y específica para la adecuada protección de infraestructuras portuarias.

La propuesta combina las funcionalidades más avanzadas de SA física con las más novedosas técnicas en prevención, detección y mitigación de ciberamenazas, incluido el uso de innovadoras técnicas de visualización para la comprensión de la situación en el ciberespacio. Asimismo, una aplicación de consciencia situacional híbrida (HSA) será capaz de determinar las potenciales consecuencias de cualquier ataque mediante la representación de los efectos cascada de toda amenaza detectada.

Así pues, la plataforma SAURON se compone de los cuatro siguientes pilares fundamentales:

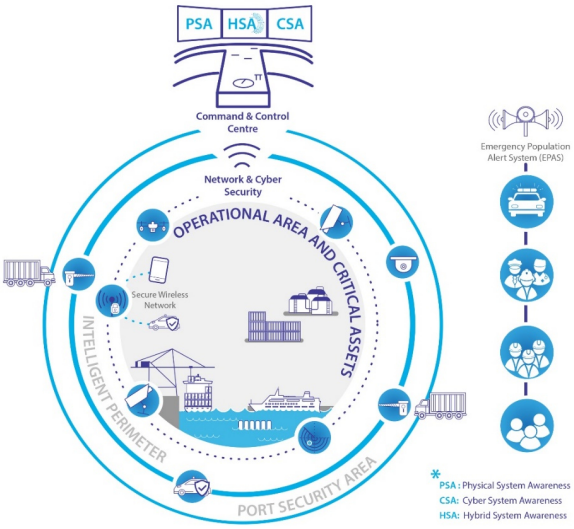


Figura 5.2: Concepto general de SAURON [3].

- ***Physical Situational Awareness* (PSA)**: un completo sistema de SA física, adaptado a las características y necesidades de los distintos puertos participantes en el proyecto, que incluye funcionalidades novedosas como la localización dinámica de recursos y activos o la gestión y monitorización de sensores, entre otras.

- ***Cyber Situational Awareness* (CSA)**: una herramienta avanzada y escalable de ciber SA capaz de detectar y prevenir amenazas así como de mitigar los efectos en caso de materializarse un ciberataque cualquiera. El sistema CSA hará uso de nuevos paradigmas de visualización para la representación del ciberespacio.

- ***Hybrid Situational Awareness* (HSA)**: un sistema de SA híbrida que recibe alarmas tanto físicas como ciber correspondientes a potenciales amenazas provenientes del mundo real y del ciberespacio respectivamente. La aplicación de HSA mostrará, mediante la representación de efectos cascada, las potenciales consecuencias de dichas amenazas en los planos tanto físico como ciber.

[3] SAURON Project, `https://www.sauronproject.eu/concept.php` [Accessed Apr. 23, 2018].

- ***Emergency Population Alert System*** **(EPAS)**: un sistema de alerta de emergencias que permita a autoridades locales, regionales y nacionales advertir tanto a los equipos de seguridad y rescate como a la población en general de la declaración de un peligro inminente, y de este modo llevar a término las acciones oportunas en respuesta al mismo.

Con el fin de validar el concepto propuesto, el proyecto contempla la realización, a lo largo del próximo año y medio, de dos demostraciones piloto complementarias en los puertos de Valencia y del Pireo en las que se evaluará la plataforma SAURON al completo en condiciones reales y en presencia de potenciales usuarios finales de la misma.

En el marco de este proyecto, donde la representación de la COP conjunta del espacio ciber-físico resulta determinante, la experiencia y conocimientos adquiridos durante el desarrollo del sistema GESTPIC por el grupo de investigación de SATRD, quien además es enteramente responsable del sistema de PSA, servirán de base fundamental para la implementación de las herramientas de CSA y HSA.

De igual modo, los desarrollos y conclusiones extraídos de SAURON relativos a la novedosa y ambiciosa propuesta en materia del cálculo de consecuencias, que pretende determinar los efectos cascada de ataques complejos sobre los dominios físico y ciber previo modelado de las dependencias estáticas y dinámicas de sus activos, podrán resultar de gran interés en el desarrollo de futuras versiones del sistema GESTPIC.

Capítulo 6

Validación de la arquitectura: HYBINT

6.1. Introducción

Pese a que el sistema GESTPIC (capítulo 4), como proyecto ya finalizado y exhaustivamente evaluado, constituye el principal caso de uso de la presente tesis doctoral para la validación de la arquitectura de HSA propuesta, se ha considerado igualmente interesante introducir la herramienta HYBINT, actualmente en fase de definición por el grupo de investigación de SATRD, como otra potencial aplicación del modelo de consciencia situacional ciber-física aquí presentado para la protección de infraestructuras críticas.

La principal motivación del sistema HYBINT no es otra que, aprovechando la experiencia adquirida a lo largo del proyecto GESTPIC en materia de CySA, desarrollar una solución de inteligencia híbrida (o mixta) por agregación tanto de fuentes adicionales de información como del conocimiento de la situación en el ciberespacio a, en esta ocasión, una herramienta de inteligencia humana preexistente.

Así pues, el presente capítulo describe, a fin de poner en contexto y de manera sintética, el proyecto CIUSAT como sistema al origen de la herramienta HYBINT para, a continuación, presentar los principales objetivos que busca alcanzar esta aplicación y, finalmente, detallar la arquitectura tentativa propuesta para la misma, los diferentes módulos que la conformarían y algunas de las que serían sus principales características.

6.2. Antecedentes y objetivos

Financiado por la *European Defence Agency* (EDA) [303] y finalizado en junio de 2016, el proyecto CIUSAT (*C-IED Interagency Unclassified Situational Awareness Tool*) [304][305] fue encargado por el Centro de Excelencia contra Artefactos Explosivos Improvisados (*Counter-Improvised Explosive Devices Centre of Excellence* (C-IED CoE)) de OTAN (Figura 6.1), quien tiene por misión [306]:

"... to provide subject matter expertise in order to support the Alliance, its Partners, and the International Community in the fight against IED and cooperate to increase security of Allied Nations and also all the troops deployed in theatres of operations, reducing or eliminating the threats from improvised explosive devices used or for use, in particular by terrorists or insurgents."

Figura 6.1: Instalaciones del C-IED CoE (Hoyo de Manzanares, Madrid) [1].

El objetivo principal de dicho proyecto no era pues otro que el desarrollo de una herramienta de SA que sirva de apoyo a las fuerzas de seguridad, tanto militares como civiles, en la prevención y respuesta frente a potenciales ataques o actividades sospechosas. Más concretamente, CIUSAT constituye una aplicación web multidispositivo (accesible desde PC y *smartphone*) destinada al intercambio de información relativa, en particular, a eventos/incidentes IED entre las distintas agencias y organizaciones involucradas (gobiernos, agentes de orden público, compañías privadas, ONGs, etc.).

En definitiva, CIUSAT se presenta como una herramienta de inteligencia capaz de mejorar la comprensión de la situación al proyectar, con un determi-

[1] NATO Counter-Improvised Explosive Devices Centre of Excellence (C-IED CoE), `http://www.emad.mde.es/CIED` [Accessed Nov. 29, 2018].

nado grado de verosimilitud, las posibles acciones futuras del enemigo u otro tipo de amenazas, mediante las siguientes tres fases:

1. La adquisición de información relativa a eventos e incidentes IED proporcionada por fuentes humanas.

2. El análisis y correlación de la información para la identificación de patrones y modelos de actuación.

3. La visualización geolocalizada de la información analizada y de la probabilidad de ocurrencia de eventos IED.

Con la seguridad como requisito fundamental del sistema, CIUSAT implementa también mecanismos para discernir entre información clasificada y no clasificada y un control de acceso de usuario para restringir, dependiendo de los privilegios asignados al mismo, las funcionalidades disponibles.

Partiendo de ese mismo enfoque, la finalidad de HYBINT sería el diseño de una solución de inteligencia para uso civil y enfocada, en este caso, a la protección de cualquier tipo de infraestructura crítica en el contexto ciber-físico actual. Con el fin de proveer un conocimiento todavía mayor de la situación en el espacio híbrido, la principal novedad de dicha aplicación respecto a CIUSAT residiría en la agregación y combinación de información de inteligencia proveniente de diferentes fuentes como, además de humanas, abiertas o sensores, como sucediese en GESTPIC, de ámbito tanto físico como ciber [307].

Así pues, HYBINT se definiría como una herramienta avanzada de inteligencia híbrida que preservaría determinadas características de diseño de CIUSAT (arquitectura escalable, diseño desacoplado en tres módulos, control de acceso, etc.) a la vez que integraría, como punto fuerte de la propuesta, métodos analíticos orientados a *Big Data* y técnicas avanzadas de representación (ya empleadas en GESTPIC) para la obtención de la adecuada HSA en un espacio único de toma de decisiones.

A modo de ejemplo, en una infraestructura crítica como podría ser una instalación portuaria, cuando el GPS de un operador de grúa lo posicionase en el área de carga en el mismo instante en el que sus credenciales estuviesen siendo empleadas para acceder a un equipo informático localizado a una distancia considerable, la información proporcionada por el responsable de seguridad que inspeccionase y reportase acerca de dichas ubicaciones, podría resultar clave para confirmar un posible ataque. En un escenario distinto, la información recogida del personal de vigilancia advirtiendo de la actitud sospechosa de una persona autorizada accediendo repetidamente a instalaciones estratégicas en

horarios no convencionales, podría ser analizada conjuntamente con su actividad reciente en la red interna de la organización a fin de determinar si estuviese actuando como infiltrado.

6.3. Arquitectura del sistema

Como muestra la Figura 6.2, el sistema HYBINT estaría basado en una arquitectura cliente-servidor con la finalidad de garantizar la escalabilidad, disponibilidad y seguridad como principales requerimientos de usuario. El núcleo de la plataforma se diseña de manera flexible y desacoplada para, al igual que en el caso de GESTPIC, facilitar la implementación de nuevas funcionalidades y la adaptación a las necesidades concretas de cada infraestructura en cuestión. Este se compondría de tres módulos principales desarrollados independientemente y siguiendo el concepto de aplicación en tres capas:

- **Módulo de adquisición de datos (DGM)**: obtiene datos relevantes relativos a la infraestructura crítica de fuentes heterogéneas de datos, tanto físicos como ciber (p. ej. sensores ambientales, cámaras de videovigilancia, analizadores de tráfico, informes del usuario, etc.), y los almacena en la base de datos del sistema.
- **Módulo de análisis de datos (DAM)**: proporciona al usuario una colección de avanzados análisis con el fin de producir información de inteligencia física, ciber o mixta (p. ej. evaluación de amenazas ciber, clasificación de instalaciones por criticidad, detección de patrones de interacciones sociales, etc.) a través del procesamiento de los datos en bruto disponibles.
- **Módulo de visualización de datos (DVM)**: facilita una HSA en tiempo real de los espacios físicos y ciber mediante la representación georreferenciada y combinada, a imagen y semejanza del enfoque aplicado en GESTPIC, de la información de inteligencia producida (p. ej. dependencias entre activos físicos y ciber, red social de individuos bajo sospecha, efectos cascada de ataques combinados, etc.).

La plataforma HYBINT, entendiéndose por ello el lado servidor de la arquitectura, consiste en una solución basada en .NET [281] y desarrollada en lenguaje C#. De nuevo, se propone inicialmente el uso de MySQL [268] como base de datos de la herramienta. Sin embargo, una vez más, se consideraría la implementación de una capa de abstracción (*Database Abstraction Layer* (DBAL)) que facilitase la integración de otros motores de base de datos desacoplando las funcionalidades propias de estos del núcleo del sistema. Desde el

módulo de administración del sistema (*System Administration Module* (SAM)), los usuarios con privilegios de administración podrían, entre otras capacidades, acceder a la completa configuración de la plataforma, administrar las diferentes fuentes de datos y usuarios del sistema, o gestionar las distintas tareas programadas.

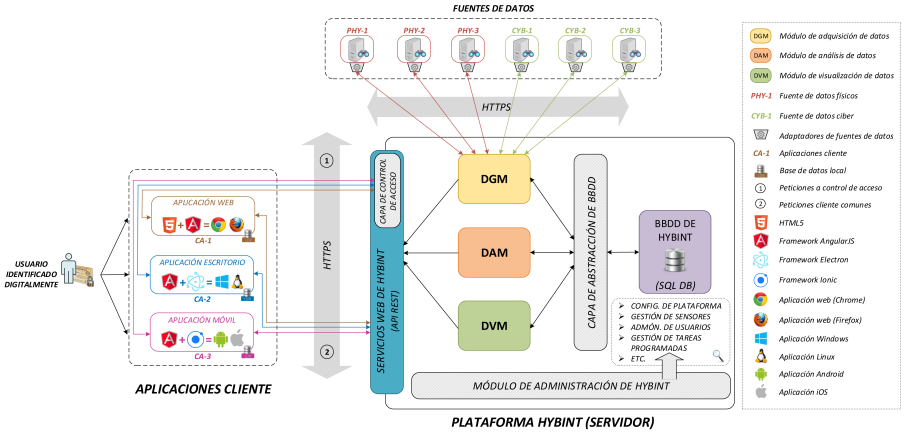


Figura 6.2: Arquitectura del sistema.

Los servicios web de la plataforma HYBINT, que estarían basados en arquitectura REST [259], se expondrían mediante un servidor web como podría ser Microsoft IIS [308]. Estos quedarían accesibles para cualquier usuario registrado en el sistema a través de tres aplicaciones cliente diferentes: aplicación web, aplicación ejecutable de escritorio y aplicación móvil. La interfaz o HMI de todas ellas consistiría en un entorno basado en web desarrollado mediante *frameworks* de JavaScript como AngularJS [309] y sobre HTML5. Las aplicaciones nativas de escritorio y móvil se compilarían gracias a *frameworks* como Electron [310] y Ionic [311] respectivamente a partir del mismo código-base. De este modo, la aplicación web sería accesible a través de cualquier navegador web actual (con soporte para HTML5) como Google Chrome o Mozilla Firefox, la aplicación de escritorio sería instalable en equipos con sistema operativo Windows y la aplicación móvil sería, por su parte, desplegable en dispositivos móviles Android o iOS.

Se emplearía HTTPS como protocolo seguro de comunicaciones entre las aplicaciones cliente y la plataforma del sistema con el fin de preservar la integridad y privacidad de los datos intercambiados. Adicionalmente, se propone la inclusión en dichos clientes de certificados de clave pública para garantizar la identidad digital de los usuarios registrados en HYBINT y su autenticación

en la herramienta. A tal fin, una capa de control de acceso (*Access Control Layer* (ACL)) sería responsable tanto de validar los certificados de usuario como de gestionar las funcionalidades disponibles según la categoría y privilegios asignados al mismo (p. ej. personal común, supervisores de área, técnicos de soporte TI, empleados de vigilancia, analistas de seguridad, etc.).

De manera adicional y como ya sucediese en CIUSAT, se desarrollaría un modo *offline* del sistema con el fin de proveer unas mínimas funcionalidades incluso no disponiéndose de conectividad alguna en el lado cliente.

Por último y a diferencia de GESTPIC, se estudiaría la utilización en esta ocasión de un modelo de datos basado en estándares de compartición como STIX [112] que facilitase en el futuro tanto el intercambio de información entre distintos servidores HYBINT como la interoperabilidad con otros sistemas de información.

6.3.1. Módulo de adquisición de datos

El módulo de adquisición de datos (*Data Gathering Module* (DGM)) es responsable de la obtención de datos de inteligencia de diversas fuentes de dominio tanto físico como ciber y su almacenamiento en la base de datos de la plataforma. Dichas fuentes de información consistirían tanto en usuarios registrados en HYBINT (p. ej. personal técnico de la infraestructura crítica, empleados de seguridad, analistas, etc.) como en sensores (físicos y ciber) encargados de reportar todo comportamiento anómalo o incidente ocurrido en las instalaciones de la infraestructura en cuestión.

Así pues y como sucediera en GESTPIC, si bien los sensores físicos harían principalmente referencia a sistemas de información (p. ej. GPS, tecnologías de control de acceso, sistemas de videovigilancia, etc.) que proporcionarían datos físicos relativos a activos físicos (p. ej. personas, vehículos, instalaciones, etc.); los sensores ciber consistirían nuevamente en herramientas de seguridad en red (p. ej. OSSIM, MISP, RTIR, etc.) que suministrarían datos ciber relativos a activos ciber (ficheros de datos, software, servicios, etc.). Por su parte, los usuarios con acceso a HYBINT aportarían, en lo que se conoce como inteligencia humana (HUMINT), datos relativos al dominio físico, ciber o a ambos como podrían ser el reconocimiento visual de personas, la detección de actividades sospechosas, la constatación de comportamientos anómalos, etc. Con el fin de enriquecer todavía más la HSA proporcionada por la herramienta, se contemplaría adicionalmente la inclusión de inteligencia de fuentes abiertas (OSINT) mediante el consumo de información pública proporcionada por medios de comunicación, redes sociales o administraciones públicas.

Como puede observarse en la Figura 6.3, el módulo DGM soportaría la entrada de datos tanto estructurados (acordes al modelo de datos de HYBINT) como no estructurados (p. ej. texto libre) y distinguiría entre métodos de adquisición automáticos y manuales.

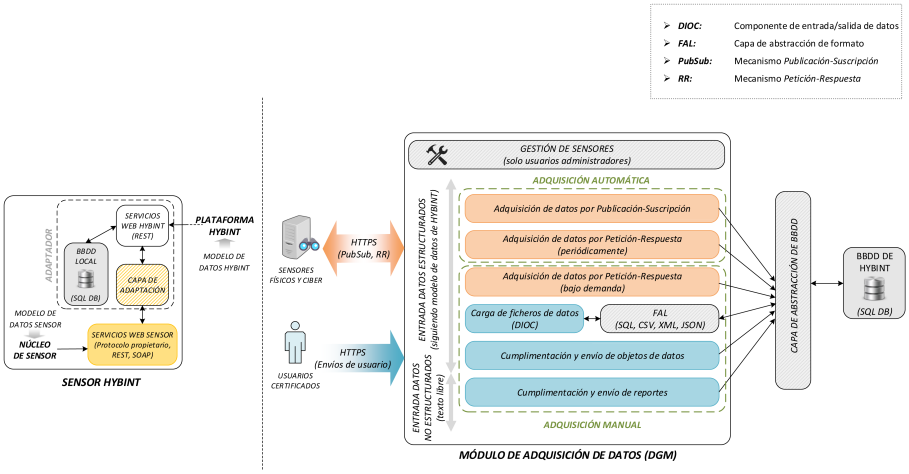


Figura 6.3: Módulo de adquisición de datos (DGM).

Por una parte, los usuarios de la plataforma contribuirían a la recolección de datos bien sea mediante la generación y envío de reportes u objetos de datos (que seguirían el modelo de datos del sistema) o mediante la carga de ficheros de datos formateados a través del componente de E/S de datos (*Data Input/Output Component* (DIOC)). En dicho caso, se implementaría una capa de abstracción de formato (*Format Abstraction Layer* (FAL)) para desacoplar el tipo de fichero (SQL, CSV, XML o JSON) del acceso a la base de datos de HYBINT. Desde el DIOC los usuarios podrían igualmente exportar en todo momento información de la base de datos a cualesquiera de dichos formatos.

De igual modo que en el caso de GESTPIC, la interoperabilidad con los sensores (físicos y ciber) desplegados en la infraestructura crítica se llevaría a cabo mediante los mecanismos de intercambio de mensajes *Request-Response* o *Publish-Subscribe* y con HTTPS como protocolo de comunicaciones entre estos y el DGM. Además, para el modelo de Petición-Respuesta, se podría optar por ejecutar las peticiones a las correspondientes fuentes de datos de manera periódica o únicamente bajo demanda del usuario.

Asimismo, únicamente los usuarios administradores estarían autorizados tanto a configurar los parámetros de acceso a los sensores existentes como a registrar otros nuevos en la plataforma.

Por último, debido a la heterogeneidad de los sensores existentes en cada tipo de infraestructura crítica, se propone el desarrollo de unos adaptadores específicos que transformen, mediante una capa de adaptación, los servicios web propios de cada uno de los sensores (basados en protocolos propietarios, operaciones REST, etc.) en servicios web basados en REST que sigan el modelo de datos de HYBINT.

Además, cuando no se dispusiese de conectividad en el lado del sensor, dichos adaptadores podrían almacenar localmente los datos en una base de datos integrada hasta poder ser transmitidos a la plataforma.

6.3.2. Módulo de análisis de datos

Con el objetivo de entregar una avanzada HSA del entorno ciber-físico, el módulo de análisis de datos (*Data Analysis Module* (DAM)) es responsable de extraer conocimiento de los datos en bruto almacenados en la plataforma. Para ello y como refleja la Figura 6.4, la interfaz del sistema pone a disposición de los usuarios de HYBINT una serie de análisis predefinidos (p. ej. evaluación de vulnerabilidades de seguridad, clasificación de instalaciones por criticidad, detección de patrones en redes sociales, análisis de redes conectadas, etc.) con el fin de generar la información de inteligencia (física, ciber o híbrida) deseada como resultado del procesamiento de los datos en *raw* correspondientes. Además, y para cualquiera de estas tareas analíticas, la plataforma permitiría seleccionar también entre programado (puntual o periódicamente) o inmediato como modo de ejecución de las mismas.

Todos los análisis de inteligencia expuestos estarían vinculados a herramientas analíticas en las que estos serían ejecutados. Dichas herramientas de análisis implementan, tal y como comentado en el capítulo 3, métodos de minería de datos [172] a través de técnicas estadísticas para extraer patrones relevantes y generar conocimiento sobre amplios conjuntos de datos (*Big Data*) con el fin de mejorar el proceso de toma de decisiones [274]. Asimismo, mediante el uso de métodos de minería de texto, el presente módulo daría también soporte al análisis de datos no estructurados como los proporcionados por el usuario del sistema en forma de reportes de inteligencia.

Estas herramientas de análisis consisten en soluciones analíticas de terceros, tanto propietarias como de libre acceso, previamente integradas en la plataforma HYBINT. Pese a que, como indicado en el capítulo 3, se propone

inicialmente el uso de IBM i2 Analyst's Notebook [188] (Figura 6.5); cabría la posibilidad de considerar igualmente la inclusión de otras soluciones también interesantes como RapidMiner [180], IBM SPSS Statistics [181] o SAP Predictive Analytics [312].

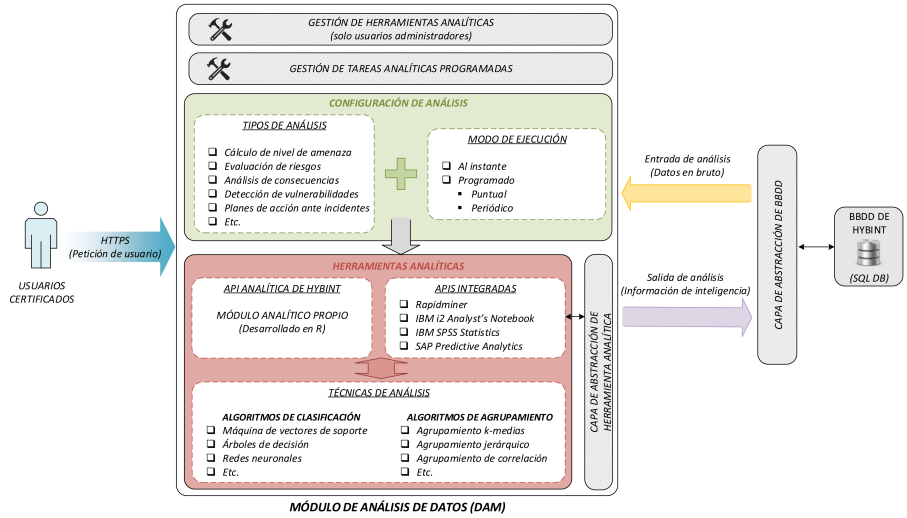
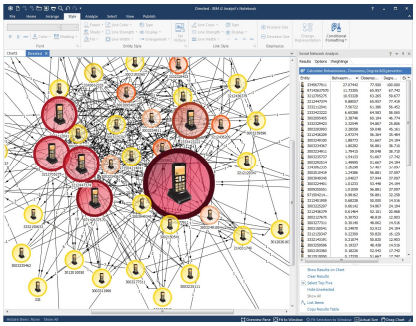


Figura 6.4: Módulo de análisis de datos (DAM).

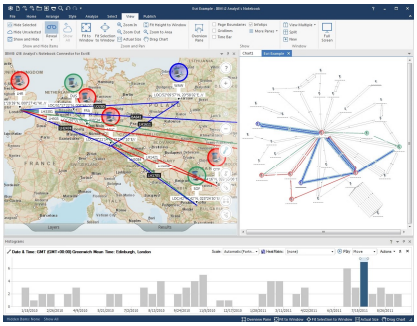
Las técnicas computacionales empleadas por estas herramientas, centradas a menudo en algoritmos basados en aprendizaje automático [173], consisten en análisis predictivos para, como se vio en el capítulo 2, estimar conductas futuras adquiriendo conocimiento a partir de datos de entrenamiento.

El acceso a las diferentes herramientas analíticas, desplegadas junto al núcleo de la plataforma HYBINT, se llevaría a cabo, dependiendo de las posibilidades que estas ofrezcan, a través de sus respectivas APIs programáticas o mediante llamadas REST a los servicios web correspondientes. Además, una capa de abstracción (*Analytic Tool Abstraction Layer* (ATAL)) se emplearía para desacoplar, en esta ocasión, la lógica interna de cada una de estas aplicaciones del núcleo del sistema.

De manera adicional, la implementación de un sub-módulo de análisis propio, con diversas funciones estadísticas y desarrollado en lenguaje R [177], vendría a complementar las capacidades ofrecidas por las herramientas externas ofreciendo análisis de datos más específicos y personalizados.



(a) Análisis de redes sociales



(b) Vistas temporales y geoespaciales

Figura 6.5: Ejemplos de uso de IBM i2 Analyst's Notebook [2].

Únicamente los usuarios administradores del sistema estarían autorizados para asignar, en la medida de lo posible, la herramienta más adecuada para la ejecución de cada uno de los análisis predefinidos así como para descartar o restaurar el uso de cualesquiera de estas. De igual modo, cada usuario de HYBINT con acceso al DAM podría modificar en todo momento la configuración de sus propias tareas de análisis.

En definitiva, cuando una de estas se iniciase, el módulo DAM interrogaría a la base de datos de HYBINT para obtener los datos necesarios y se los serviría a la herramienta analítica en cuestión. La información de inteligencia resultante del procesamiento correspondiente quedaría posteriormente registrada en la base de datos a fin de estar disponible para su representación en el módulo de visualización.

6.3.3. Módulo de visualización de datos

El módulo de visualización de datos (*Data Visualization Module* (DVM)) tiene por objetivo, como ya se vio en capítulos anteriores, el proveer la adecuada HSA al usuario de la plataforma en un espacio único de visualización. Como ilustra a título tentativo la Figura 6.6, el HMI del presente módulo tendría un aspecto similar al de la aplicación GESTPIC pero implementado, en esta ocasión y como indicado anteriormente, como un entorno web multiplataforma.

[2] IBM i2 Analyst's Notebook, `https://www.ibm.com/us-en/marketplace/analysts-notebook` [Accessed Apr. 23, 2018].

Se trataría, por tanto, de hacer nuevamente uso de las técnicas avanzadas de representación propuestas en esta tesis doctoral pero aplicadas, esta vez, a la información de inteligencia física, ciber e híbrida proporcionada por el DAM. En este sentido, la presente herramienta pretende ir un paso más allá que el sistema GESTPIC al combinar, en un espacio único de toma de decisiones, la representación de información ciber-física (como este último proporciona) con la representación de información proveniente de otras fuentes de inteligencia como las humanas o abiertas.

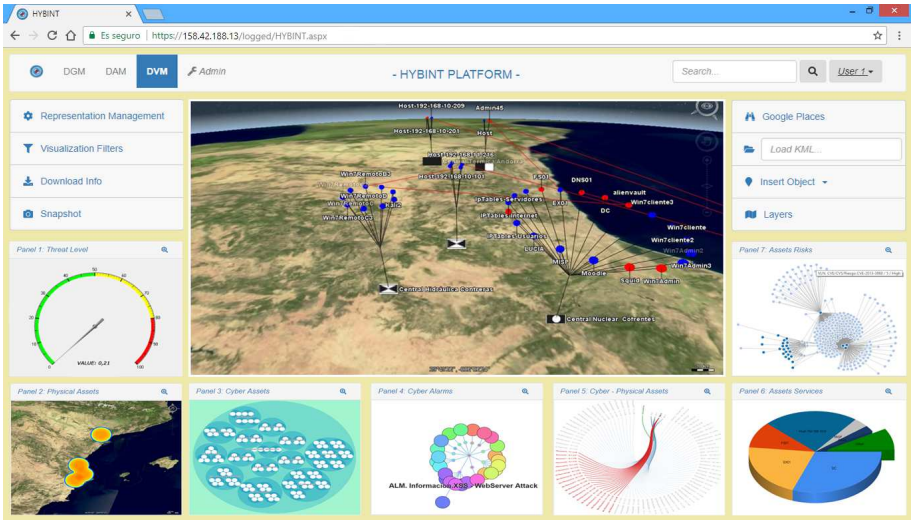


Figura 6.6: Módulo de visualización de datos (DVM).

Tal y como sucediese en el caso de uso anterior, la interfaz del DVM estaría fundamentalmente compuesta por un mapa geográfico principal (GIS basado en web) y una serie de paneles gráficos alrededor del mismo para la representación combinada y en tiempo real de la información de inteligencia producida. Como señalado en el capítulo 3, Luciad [210] y Cesium [218] conformarían las herramientas geoespaciales inicialmente integradas en el sistema así como Microsoft Chart Controls [225] y Data-Driven Documents [230] las bibliotecas para la generación de grafos y diagramas.

Una vez más, con la total flexibilidad en la representación de cualquier tipo de información almacenada como requisito fundamental y diferenciador de HYBINT, la interfaz del DVM dispondría de un menú, al igual que GESTPIC, para la completa gestión de las representaciones desde la que poder definir

cualquier tipo de consulta a la base de datos (bien sea relativa a los datos en bruto almacenados o a los resultados de análisis de inteligencia efectuados por el DAM) así como configurar el tipo de representación correspondiente (georreferenciada sobre GIS (grafo 3D, KML, mapa de calor) o grafo/diagrama clásico o avanzado) y el panel de visualización deseado (mapa principal o paneles gráficos).

Por último y adicionalmente a características ya implementadas en el sistema GESTPIC como la gestión de capas o el filtrado de la visualización, la plataforma incluiría una serie de funcionalidades extra con el fin de enriquecer todavía más las capacidades ofrecidas por el DVM tales como consultas a la base de datos de Google Places [276], la inserción de objetos georreferenciados en el mapa (puntos, líneas/polilíneas, polígonos, etc.) o la exportación tanto de capturas de pantalla como de todo tipo de información generada (reportes de inteligencia en formato texto, grafos/diagramas en formato imagen o datos geoespaciales en formato KML).

6.3.4. Características adicionales

Modo offline

El sistema HYBINT, definido como solución multiplataforma, garantizaría el requerimiento de escalabilidad al ser accesible, a través de los servicios web expuestos, desde un amplio número de dispositivos con conectividad (PCs, *tablets*, *smartphones*, etc.). Sin embargo, el acceso a la plataforma podría no estar siempre asegurado dependiendo de las condiciones de red en el lado cliente.

De este modo y con el fin de mejorar el requerimiento de disponibilidad, cuando no se dispusiese de conexión alguna en las aplicaciones cliente, estas conmutarían automáticamente a un modo *offline* en el que únicamente estarían habilitadas las funcionalidades vinculadas a datos locales. De manera transparente, los datos obtenidos tanto de ficheros cargados como de reportes cumplimentados quedarían almacenados localmente en una muy sencilla base de datos integrada en las aplicaciones cliente (Figura 6.2) hasta que un servicio local reestableciese automáticamente el modo principal de HYBINT una vez estuviese de nuevo accesible la plataforma.

Perfiles de acceso

En lo que al requerimiento de seguridad se refiere, más allá del uso de protocolos seguros de comunicaciones (HTTPS) y certificados de clave pública, se sugiere también la definición de una serie de niveles de acceso para, al igual que en la herramienta CIUSAT, restringir las funcionalidades disponibles de acuerdo con el rango o posición del usuario de HYBINT en su correspondiente organización (en este caso, infraestructura crítica).

Así pues, la Tabla 6.1 resume los distintos perfiles de acceso a la plataforma propuestos y sus respectivas capacidades principales.

Nivel	Módulos accesibles	Capacidades principales
1	DGM	Generación de nuevos reportes y carga de ficheros de datos
2		Nivel 1 + Gestión de reportes propios
3		Nivel 1 + Gestión completa de reportes
4	DGM + DAM	Nivel 2 + Análisis sobre datos propios
5		Nivel 3 + Análisis sobre todos los datos y programación de tareas analíticas
6	DGM + DAM + DVM	Nivel 4 + Representación de resultados de análisis propios
7		Nivel 5 + Representación de resultados de todos los análisis
8	DGM + DAM + DVM	Nivel 7 + Capacidades de administración

Tabla 6.1: Niveles de acceso al sistema y capacidades asociadas.

Por defecto, el mínimo nivel de acceso sería inicialmente asignado a todo nuevo usuario registrado en HYBINT; y únicamente los usuarios administradores del sistema estarían habilitados tanto para otorgar los correspondientes privilegios a cada uno de ellos como para gestionar los diferentes perfiles existentes bien sea modificándolos o creando otros nuevos.

Control de confianza

Por último, resultaría igualmente interesante la implementación en la plataforma de un sistema de control de confianza tanto de los usuarios con bajo perfil de acceso como de la información aportada por cada uno de ellos. De este modo y de manera transparente para estos últimos, se obtendría una información de inteligencia todavía más precisa y acertada al ponderar el análisis de la misma por el *rating* asociado a esta en todo momento.

A tal fin, HYBINT dispondría de una funcionalidad desde la que únicamente los usuarios con un determinado nivel de privilegios podrían valorar, tanto mediante comentarios como numéricamente, la calidad y fiabilidad de los diversos reportes generados como de sus respectivos autores.

Capítulo 7

Conclusiones

7.1. Conclusiones finales

En la presente tesis doctoral se ha analizado las implicaciones que conlleva, para las infraestructuras críticas, el desarrollo hoy en día de actividades en el ciberespacio y la necesidad, por consiguiente, de nuevas soluciones en el área de la CySA que garanticen la seguridad de las mismas en el contexto ciber-físico. A continuación, se ha presentado una arquitectura genérica de HSA orientada a la protección de todo tipo de infraestructura crítica en el entorno híbrido actual. Dicho modelo ha sido posteriormente aplicado a dos casos de uso distintos en el ámbito del *Cyber Command & Control* a través de los sistemas GESTPIC y HYBINT.

Los siguientes apartados tienen por objeto exponer las principales conclusiones extraídas a lo largo de esta investigación.

7.1.1. Conclusiones generales

Estado del arte

- El momento tecnológico presente, con conceptos como el *Big Data*, el IoT o la inteligencia artificial a la cabeza, exige percibir cada vez más los espacios físico y lógico como un todo único. Esta realidad implica infinidad de posibilidades para las organizaciones pero también nuevos riesgos que han de ser debidamente gestionados.

- En el caso de infraestructuras críticas, necesariamente ligadas entre sí para el cumplimiento de sus funciones, los riesgos son aun mayores pues el ataque a una de ellas puede causar efectos cascada sobre otras muchas.
- Sin embargo, el número de ciberataques sigue multiplicándose año a año, siendo estos cada vez más heterogéneos y complejos. Tras ellos, se esconden múltiples actores con motivaciones muy diversas; y sus consecuencias, más allá del factor económico o del robo de información, pueden incluso alcanzar la pérdida de vidas humanas.
- Con el propósito de afrontar de forma eficiente la protección de infraestructuras críticas en el marco actual, son por tanto imprescindibles nuevas y avanzadas soluciones que, aplicando el concepto de CySA a herramientas tradicionales de C2, proporcionen en tiempo real la adecuada SA híbrida (HSA) del entorno ciber-físico en un espacio único de actuación.
- En este contexto, dispositivos convencionales de seguridad como antivirus, *firewalls* o IDS resultan por sí solos insuficientes al estar pensados para una defensa más bien preventiva o pasiva. Herramientas más completas como los SIEM, al nutrirse de la información aportada por todos ellos, suponen un enfoque más adecuado para la prevención de posibles ataques mediante la detección de anomalías o actividades sospechosas.
- Por su parte, algunas de las soluciones SCADA más recientes, como subconjunto de los tradicionales sistemas ICS, integran ya hoy por hoy muchas de estas herramientas de seguridad. Si bien y pese a emplear tecnologías de lo más actuales como servicios *cloud* o IoT, estos siguen en su mayoría enfocados solo al ámbito industrial.
- En el ámbito de la inteligencia, el análisis de datos implica técnicas analíticas basadas en *data mining* y *machine learning* para la extracción de características y la predicción de estados futuros. Integrar en dicho proceso otras fuentes de información como las humanas o abiertas siempre contribuirá a un mejor conocimiento de la situación. En el caso particular de sistemas de seguridad, dichos análisis están habitualmente centrados en el análisis de riesgos de los activos de la infraestructura.
- Contrariamente a visualizaciones de la información que a menudo resultan poco intuitivas y útiles al operador, se imponen técnicas avanzadas de *visual analytics* que incrementen instantáneamente la percepción humana de la situación para la mejora en la toma de decisiones. Debido a su continua evolución, siguen destacando en este punto los más completos sistemas GIS y servicios de *web mapping* para la representación geolocalizada y en tiempo real de la información ciber-física.

- En lo que a grafos y diagramas dinámicos se refiere, son también muchas las alternativas existentes que permiten resaltar, de manera muy atractiva y a golpe de vista, las relaciones entre la información representada.
- No obstante, cuando la cantidad de información a representar es desmedida, el espacio bidimensional se muestra insuficiente. En este caso, la representación mediante grafos 3D resulta la mejor opción y la visualización inmersiva, mediante técnicas como AR o VR, el mejor vehículo para navegar e interactuar entre complejas estructuras de datos.

Especificación de la arquitectura

- La principal aportación de la presente tesis doctoral ha sido la arquitectura propuesta de SA ciber-física para la defensa ágil y eficiente de infraestructuras críticas en el entorno híbrido.
- El modelo ha sido definido de manera genérica con el fin de adaptarse a las necesidades de todo tipo de infraestructura crítica y de ser aplicable a distintos casos de uso de *Cyber Command & Control*.
- La arquitectura, desarrollada de forma flexible para facilitar la integración de posteriores requerimientos funcionales y de usuario, consta esencialmente de cuatro módulos principales: adquisición de datos, fusión de datos, análisis de datos y visualización de información.
- El módulo de adquisición de datos se comunica con diversas fuentes heterogéneas de datos para la obtención de toda información relativa a activos físicos y ciber. La interoperabilidad con dichos sistemas externos se efectúa, según el caso, mediante mecanismos propios de comunicación o llamadas REST estándar.
- La información ciber y física queda relacionada, siguiendo un modelo de datos específico por cada caso de aplicación, en el módulo de fusión de datos. Pese a que se opta inicialmente por el uso de MySQL como base de datos, el diseño desacoplado de la arquitectura posibilita la futura incorporación de otro tipo de motores.
- El módulo de análisis de datos depende del tipo de sistema al que se vaya a aplicar la arquitectura propuesta. En el caso de GESTPIC, atiende a capacidades como el análisis de riesgos y de consecuencias o la estimación del nivel de amenaza. En el caso de HYBINT, consiste en la ejecución de análisis predefinidos sobre el conjunto de datos disponibles para la producción de información de inteligencia.

- El módulo de visualización emplea técnicas innovadoras de representación para proveer la HSA del entorno ciber-físico en un espacio único de toma de decisiones. En particular, se distingue la representación georreferenciada sobre GIS, el uso de diagramas y grafos avanzados y la visualización inmersiva mediante VR.

7.1.2. Sistema GESTPIC

- El objetivo esencial de GESTPIC es el desarrollo de una herramienta de visualización que proporcione en tiempo real la COP conjunta de los dominios físico y lógico para la adecuada protección de infraestructuras críticas en el contexto actual.

- Dotado con las tradicionales características de un sistema clásico de SA, el responsable de seguridad es capaz de adquirir una consciencia situacional apropiada del entorno híbrido (HSA), proyectar dicha comprensión a futuro para predecir el curso de la situación y poder, de este modo, tomar las decisiones oportunas.

- El sistema ofrece tres niveles de vista diferentes, con distintos grados de detalle, dependiendo de las necesidades de información del operador en cuestión y, por ende, de su rol en la organización: nivel estratégico, nivel operacional y nivel técnico.

- GESTPIC hace inicialmente uso de OSSIM, MISP y RTIR como fuentes de datos ciber así como de cualquier tipo de sensor desplegado en el espacio físico como fuente de datos físicos. Un módulo de configuración permite la gestión remota del acceso a todos estos sistemas externos.

- Apoyado por la herramienta externa PILAR, las capacidades analíticas que ofrece el módulo de análisis y correlación de datos incluyen el estado general de riesgos, el estado de riesgo por activo, el análisis de consecuencias y el nivel de amenaza global.

- El sistema integra Luciad y Cesium como soluciones GIS para la representación tridimensional de conjuntos complejos de datos, bibliotecas *open source* para la generación de diagramas interactivos y, como aporte novedoso, dispositivos VR para la navegación en entorno inmersivo.

- La solución ha sido implementada en entorno .NET como una aplicación ejecutable desarrollada en lenguaje C#. A través de su HMI, el operador puede acceder también a la completa configuración del sistema y a la

gestión tanto de la información almacenada como de las distintas representaciones disponibles.

- Un prototipo final del sistema GESTPIC fue exhaustivamente evaluado, tanto técnica como operativamente, mediante una serie de tests funcionales llevados a cabo en escenarios de uso tanto simulados como reales específicamente confeccionados a tal fin.

- Los conocimientos y resultados derivados del desarrollo de este último están siendo actualmente empleados en el proyecto europeo SAURON, centrado en la protección de infraestructuras portuarias, para el diseño e implementación de sus herramientas de CSA y HSA.

7.1.3. Sistema HYBINT

- La principal finalidad de HYBINT es el diseño de una solución avanzada de inteligencia basada en la agregación y combinación de información de fuentes distintas de inteligencia e igualmente orientada a la protección de infraestructuras críticas.

- HYBINT se erige como una herramienta de inteligencia híbrida que proporcionaría, por integración tanto de información proveniente de sensores como de fuentes abiertas o humanas y mediante el uso de métodos analíticos para *Big Data*, un conocimiento todavía mayor de la situación en el entorno ciber-físico.

- Con el fin de cumplir con los requisitos de escalabilidad y disponibilidad, el sistema HYBINT respondería a una arquitectura cliente-servidor compuesta por tres módulos centrales desarrollados nuevamente de manera desacoplada y flexible.

- Los servicios web de la plataforma estarían basados en arquitectura REST, la solución contaría con tres aplicaciones cliente distintas (de escritorio, web y móvil) y, con la seguridad como requerimiento fundamental, se emplearían tanto protocolos de comunicación cifrada como certificados de clave pública que garanticen la identidad de los usuarios.

- Mediante un módulo de adquisición de datos, el sistema consumiría y almacenaría información proporcionada por sensores físicos y ciber pero también, y como aspecto novedoso, de otras fuentes de inteligencia como las humanas (usuarios de la plataforma) o las abiertas (administraciones públicas, medios de comunicación, etc.).

- HYBINT facilitaría, a través de su módulo de análisis de datos, una serie de análisis avanzados con el fin de generar información de inteligencia física, ciber o híbrida que resulte de interés al usuario. Las herramientas analíticas usadas para ello emplean *data mining* y *machine learning* para detectar patrones relevantes y predecir comportamientos futuros.

- Tanto visualizaciones geolocalizadas sobre GIS como grafos y diagramas serían de nuevo utilizados para la representación, en este caso, de información de inteligencia. El módulo de visualización permitiría, además y entre otras funcionalidades, el acceso a bases de datos de terceros o la exportación de la información generada en múltiples formatos.

- La solución dispondría además de un modo *offline* con el objetivo de proveer unas capacidades mínimas al usuario cuando no se dispusiese de conectividad en el lado cliente. En este caso, la información quedaría temporalmente almacenada en las aplicaciones cliente hasta poder ser transmitida a la plataforma HYBINT.

- La plataforma implementaría también un conjunto de perfiles distintos de acceso con la finalidad de presentar las funcionalidades disponibles para cada usuario en cuestión en función de sus privilegios o, dicho de otro modo, de su rol en su correspondiente organización.

7.2. Líneas futuras de investigación

Al término de la presente tesis doctoral, se plantean numerosas áreas de estudio en las que ahondar como ampliación al trabajo aquí llevado a cabo.

A continuación, se señalan algunas de las líneas de investigación más destacables a desarrollar en el futuro.

- La utilización de bases de datos relacionales podría resultar insuficiente a la hora de gestionar volúmenes masivos de datos. Alternativas NoSQL tales como MongoDB [273] o Apache Cassandra [271] proporcionarían mayores prestaciones en entornos *Big Data* al ofrecer mayor escalabilidad y flexibilidad. Soluciones como Elasticsearch [313] optimizarían además la búsqueda de información por su eficiente capacidad de indexación.

- Las fuentes de datos ciber hoy en día existentes emplean protocolos y formatos muy diversos, tanto propietarios como estándar, para la compartición de información. Con el fin de favorecer la interoperabilidad de GESTPIC y HYBINT con aquellas que soporten protocolos estándar de

intercambio de información ciber como STIX [112] o SCAP [117], sería conveniente el diseño de adaptadores específicos por cada uno de estos.

- Resultaría también interesante el desarrollo de capacidades de federación con el fin de intercambiar información, mediante técnicas de replicación, entre distintos nodos GESTPIC o HYBINT. En este sentido, cabría explorar tecnologías altamente eficientes basadas en mecanismos de comunicación *Publish-Subscribe* como RabbitMQ [314] o Apache Kafka [315].

- El análisis de riesgos del sistema GESTPIC combina la información, de naturaleza estática, producida por la herramienta externa PILAR con la recibida en tiempo real relativa a eventos e incidentes. Se propone mejorar dicha funcionalidad confiriéndole mayor dinamismo al considerar las condiciones cambiantes del entorno en el cálculo de riesgos.

- De manera similar, la capacidad de análisis de consecuencias de GESTPIC podría verse asimismo perfeccionada con los resultados que deriven en este sentido del proyecto SAURON. En efecto, dado un evento en particular, un conocimiento más completo y preciso de la situación sería posible considerando la propagación en cascada de efectos que causaría una acción física, ciber o combinada sobre el conjunto del sistema.

- Sería igualmente recomendable la inclusión en GESTPIC de mecanismos de seguridad, como ya sucediese en HYBINT, tales como la solicitud de credenciales de inicio de sesión, la implementación de diferentes perfiles de acceso o el requerimiento de certificados de clave pública.

- En lo que concierne al sistema HYBINT, se hace ante todo necesaria la completa evaluación, tanto técnica como operativa, de un prototipo del mismo, una vez finalizada su implementación, en un escenario real de uso que deberá ser específicamente definido para este propósito.

- Además, se considera que el despliegue de servidores de réplica de HYBINT a modo de arquitectura distribuida permitiría incrementar la alta disponibilidad y la tolerancia a fallos al encaminar equitativamente el tráfico de peticiones entre los mismos.

- Por último, se sugiere la integración en HYBINT de soluciones analíticas adicionales como RapidMiner [180] o SAP Predictive Analytics [312] como complemento a las capacidades brindadas por IBM i2 Analyst's Notebook [188]. Un sistema de cola de mensajes que gestionase el conjunto de peticiones mitigaría además posibles problemas de escalabilidad en el acceso a los servicios de aquellas con licencia propietaria.

Referencias

[1] M. Wollschlaeger, T. Sauter, and J. Jasperneite, "The Future of Industrial Communication: Automation Networks in the Era of the Internet of Things and Industry 4.0," *IEEE Industrial Electronics Magazine*, vol. 11, no. 1, pp. 17–27, Mar. 2017.

[2] L. Monostori, "Cyber-physical Production Systems: Roots, Expectations and R&D Challenges," in *Proceedings of the 47th CIRP Conference on Manufacturing Systems*, vol. 17, Windsor, Canada, Apr. 28–30, 2014, pp. 9–13.

[3] B. Genge, C. Siaterlis, and M. Hohenadel, "Impact of Network Infrastructure Parameters to the Effectiveness of Cyber Attacks Against Industrial Control Systems," *International Journal of Computers Communications & Control*, vol. 7, no. 4, pp. 674–687, Nov. 2012.

[4] A. F. Leite, L. Weigang, J. A. Fregnani, and I. R. de Oliveira, "Big data management and processing in the context of the system wide information management," in *2017 IEEE 20th International Conference on Intelligent Transportation Systems (ITSC)*, Yokohama, Japan, Oct. 16–19, 2017, pp. 1–8.

[5] B. Cheng, J. Zhang, G. P. Hancke, S. Karnouskos, and A. W. Colombo, "Industrial Cyberphysical Systems: Realizing Cloud-Based Big Data Infrastructures," *IEEE Industrial Electronics Magazine*, vol. 12, no. 1, pp. 25–35, Mar. 2018.

[6] A. W. Colombo *et al.*, Eds., *Industrial Cloud-Based Cyber-Physical Systems: The IMC-AESOP Approach*, 1st ed. Cham: Springer International Publishing, 2014.

[7] G. Kumar and K. Kumar, "The Use of Artificial-Intelligence-Based Ensembles for Intrusion Detection: A Review," *Applied Computational Intelligence and Soft Computing*, vol. 2012, pp. 1–20, Jul. 2012.

[8] M. A. Ferrag, L. A. Maglaras, H. Janicke, J. Jiang, and L. Shu, "Authentication Protocols for Internet of Things: A Comprehensive Survey," *Security and Communication Networks*, vol. 2017, pp. 1–41, Nov. 2017.

[9] M. Conti *et al.*, "Looking ahead in pervasive computing: Challenges and opportunities in the era of cyber–physical convergence," *Pervasive and Mobile Computing*, vol. 8, no. 1, pp. 2–21, Feb. 2012.

[10] H. Zhuge, "Semantic linking through spaces for cyber-physical-socio intelligence: A methodology," *Artificial Intelligence*, vol. 175, no. 5-6, pp. 988–1019, Apr. 2011.

[11] K. Coffey, R. Smith, L. Maglaras, and H. Janicke, "Vulnerability Analysis of Network Scanning on SCADA Systems," *Security and Communication Networks*, vol. 2018, pp. 1–21, Mar. 2018.

[12] European Political Strategy Centre (EPSC). European Commission. [Online]. Available: http://ec.europa.eu/epsc [Accessed May 8, 2018].

[13] European Political Strategy Centre (EPSC), "Building an Effective European Cyber Shield: Taking EU Cooperation to the Next Level," *EPSC Strategic Notes*, no. 24, May 2017.

[14] Department of Homeland Security (DHS). U.S. Government. [Online]. Available: https://www.dhs.gov [Accessed May 8, 2018].

[15] United States Computer Emergency Readiness Team (US-CERT), "Alert (TA17-181A) Petya Ransomware," US-CERT, Washington D.C., United States, Tech. Rep. TA17-181A, 2017.

[16] United States Computer Emergency Readiness Team (US-CERT), "Alert (TA17-132A) Indicators Associated With WannaCry Ransomware," US-CERT, Washington D.C., United States, Tech. Rep. TA17-132A, 2017.

[17] S. Mohurle and M. Patil, "A brief study of Wannacry Threat: Ransomware Attack 2017," *International Journal of Advanced Research in Computer Science (IJARCS)*, vol. 8, no. 5, pp. 1938–1940, Jun. 2017.

[18] Centro Criptológico Nacional (CCN-CERT). Centro Nacional de Inteligencia (CNI). [Online]. Available: https://www.ccn-cert.cni.es [Accessed Apr. 23, 2018].

[19] Centro Nacional de Inteligencia (CNI). Ministerio de Defensa. [Online]. Available: https://www.cni.es [Accessed May 8, 2018].

[20] Centro Criptológico Nacional (CCN-CERT), "Ciberamenazas y Tendencias - Resumen Ejecutivo," CCN-CERT, Madrid, Spain, Tech. Rep. IA-09/16, 2016.

[21] Centro Criptológico Nacional (CCN-CERT), "Ciberamenazas y Tendencias - Resumen Ejecutivo," CCN-CERT, Madrid, Spain, Tech. Rep. IA-16/17, 2017.

[22] J. Healey, "Winning and losing in cyberspace," in *2016 8th International Conference on Cyber Conflict (CyCon)*, Tallinn, Estonia, May 2016, pp. 37–49.

[23] Kaspersky. Kaspersky Lab. [Online]. Available: https://www.kaspersky.com [Accessed May 8, 2018].

[24] Kaspersky Lab, "Measuring Financial Impact of IT Security on Businesses," *IT Security Risks Report Series*, 2016.

[25] D. DiMase, Z. A. Collier, K. Heffner, and I. Linkov, "Systems engineering framework for cyber physical security and resilience," *Environment Systems and Decisions*, vol. 35, no. 2, pp. 291–300, Jun. 2015.

[26] Y. Deng, L. Song, Z. Zhou, and P. Liu, "Complexity and Vulnerability Analysis of Critical Infrastructures: A Methodological Approach," *Mathematical Problems in Engineering*, vol. 2017, pp. 1–12, Oct. 2017.

[27] GESTOP - Sistema de Gestión de Operativos. TR Sistemas. [Online]. Available: http://www.trsistemas.com/productos.php#gestop [Accessed Apr. 23, 2018].

[28] Department of Defense (DoD). U.S. Government. [Online]. Available: https://www.defense.gov [Accessed May 11, 2018].

[29] *Dictionary of Military and Associated Terms*, Joint Chiefs Of Staff, Office Secretary of Defense, U.S. Department of Defense, JP 1-02, 2016.

[30] J. R. Boyd, "The OODA Loop," A Discourse on Winning and Losing. 1976.

[31] North Atlantic Treaty Organization (NATO). [Online]. Available: https://www.nato.int [Accessed May 12, 2018].

[32] *NATO Glossary of Terms and Definitions*, NATO Standardization Office (NSO), APP-06, 2017.

[33] E. Cubeiro, "Los sistemas de mando y control: una visión histórico-prospectiva," *Boletín de Información del Ministerio de Defensa*, vol. 271, pp. 31–56, 2001.

[34] D. S. Alberts, J. J. Garstka, R. E. Hayes, and D. A. Signori, *Understanding Information Age Warfare*. Washington D.C.: CCRP Publication Series, 2001.

[35] N. A. Stanton, P. R. G. Chambers, and J. Piggott, "Situational awareness and safety," *Safety Science*, vol. 39, no. 3, pp. 189–204, Dec. 2001.

[36] M. J. Adams, Y. J. Tenney, and R. W. Pew, "Situation Awareness and the Cognitive Management of Complex Systems," *Human Factors*, vol. 37, no. 1, pp. 85–104, Mar. 1995.

[37] K. Smith and P. A. Hancock, "Situation Awareness Is Adaptive, Externally Directed Consciousness," *Human Factors*, vol. 37, no. 1, pp. 137–148, Mar. 1995.

[38] G. Z. Bedny and D. Meister, "Theory of Activity and Situation Awareness," *International Journal of Cognitive Ergonomics*, vol. 3, no. 1, pp. 63–72, Jan. 1999.

[39] M. R. Endsley, "Design and Evaluation for Situation Awareness Enhancement," in *Proceedings of the Human Factors Society Annual Meeting*, vol. 32, no. 2, 1988, pp. 97–101.

[40] M. R. Endsley, "Toward a Theory of Situation Awareness in Dynamic Systems," *Human Factors*, vol. 37, no. 1, pp. 32–64, Mar. 1995.

[41] M. R. Endsley, "Situation Awareness," in *Handbook of Human Factors and Ergonomics*, G. Salvendy, Ed. Hoboken: John Wiley & Sons, Inc., 2012, ch. 19, pp. 553–568.

[42] G. Conti, J. Nelson, and D. Raymond, "Towards a cyber common operating picture," in *2013 5th International Conference on Cyber Conflict (CyCon)*, Tallinn, Estonia, Jun. 4–7, 2013, pp. 1–17.

[43] M. R. Endsley, "Situation awareness global assessment technique (SAGAT)," in *Proceedings of the IEEE 1988 National Aerospace and Electronics Conference*, vol. 3, Dayton, United States, May 23–27, 1988, pp. 789–795.

[44] Centro Criptológico Nacional (CCN-CERT), "Ciberamenazas y Tendencias," CCN-CERT, Madrid, Spain, Tech. Rep. IA-16/17, 2017.

[45] Microsoft Corporation, "Microsoft Security Intelligence Report," *Microsoft Security*, vol. 21, 2016.

[46] Cisco Systems, "Cisco 2017 Annual Cybersecurity Report," *Cisco Cybersecurity Reports*, 2017.

[47] Verizon, "2016 Data Breach Investigations Report: 89 % of breaches had a financial or espionage motive," *Verizon Resource Center*, 2016.

[48] Neustar. Neustar, Inc. [Online]. Available: https://www.home.neustar [Accessed May 24, 2018].

[49] Neustar, Inc., "Worldwide DDoS Attacks & Protection Report: A Steady State of Threats in the Connected World," *Neustar Reports*, 2016.

[50] Akamai. Akamai Technologies, Inc. [Online]. Available: https://www.akamai.com [Accessed May 24, 2018].

[51] Akamai Technologies, Inc., "Q4 2016 State of the Internet / Security Report," *Akamai Research - The State of the Internet*, 2017.

[52] SecureWorks, Inc., "2016 Underground Hacker Marketplace Report," *SecureWorks Reports*, 2016.

[53] Dropbox. Dropbox, Inc. [Online]. Available: https://www.dropbox.com [Accessed May 24, 2018].

[54] Google Docs. Google LLC. [Online]. Available: https://docs.google.com [Accessed May 24, 2018].

[55] Pinterest. Pinterest. [Online]. Available: https://www.pinterest.com [Accessed May 24, 2018].

[56] B. Anderson. (2016, Jan. 25) Hiding in Plain Sight: Malware's Use of TLS and Encryption. [Online]. Available: https://blogs.cisco.com/security/malwares-use-of-tls-and-encryption [Accessed May 25, 2018].

[57] Android. Google LLC. [Online]. Available: https://www.android.com [Accessed May 24, 2018].

[58] National Cyber Security Centre, "Cyber Security Assessment Netherlands (CSAN) 2016," *Cyber Security Assessment Netherlands*, 2016.

[59] Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (ONTSI), "Estudio sobre la Ciberseguridad y Confianza en los hogares españoles," ONTSI, Madrid, Spain, Tech. Rep. Enero-Junio 2016, Nov. 2016.

[60] Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (ONTSI), "Estudio sobre la Ciberseguridad y Confianza en los hogares españoles," ONTSI, Madrid, Spain, Tech. Rep. Julio-Diciembre 2016, Apr. 2017.

[61] Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (ONTSI), "Estudio sobre la Ciberseguridad y Confianza en los hogares españoles," ONTSI, Madrid, Spain, Tech. Rep. Enero-Junio 2017, Oct. 2017.

[62] Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (ONTSI). Ministerio de Energía, Turismo y Agenda Digital. [Online]. Available: http://www.ontsi.red.es/ontsi/es [Accessed May 25, 2018].

[63] B. Hau, T. Lee, and J. Homan. (2015, Sep. 15) SYNful Knock - A Cisco router implant - Part I. [Online]. Available: https://www.fireeye.com/blog/threat-research/2015/09/synful_knock_-_acis.html [Accessed May 25, 2018].

[64] National Cyber Security Centre, "Cyber Security Assessment Netherlands (CSAN) 2015," *Cyber Security Assessment Netherlands*, 2015.

[65] Ericsson, "Ericsson Mobility Report - June 2016," *Ericsson Mobility Reports*, 2016.

[66] European Commission, "Special Eurobarometer 423: Cyber security," *European Union Open Data Portal*, Mar. 2015.

[67] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. Official Journal of the European Union, 23 December 2008, no. 345, pp. 75-82.

[68] Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas. Boletín Oficial del Estado, 29 de abril de 2011, núm. 102, pp. 43370-43380.

[69] Critical infrastructure (CI). European Commission. [Online]. Available: https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure [Accessed Apr. 22, 2018].

[70] European Programme for Critical Infrastructure Protection (EPCIP). European Commission. [Online]. Available: https://ec.europa.eu/home-affairs/content/european-programme-critical-infrastructure-protection-epcip [Accessed Apr. 26, 2018].

[71] Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC). Secretaría de Estado de Seguridad. [Online]. Available: http://www.cnpic.es [Accessed May 6, 2018].

[72] Secretaría de Estado de Seguridad. Ministerio del Interior. [Online]. Available: http://www.interior.gob.es/el-ministerio/funciones-y-estructura/secretaria-de-estado-de-seguridad [Accessed May 6, 2018].

[73] Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas. Boletín Oficial del Estado, 21 de mayo de 2011, núm. 121, pp. 50808-50826.

[74] C. Alcaraz and S. Zeadally, "Critical infrastructure protection: Requirements and challenges for the 21st century," *International Journal of Critical Infrastructure Protection*, vol. 8, pp. 53–66, Jan. 2015.

[75] European Union Agency for Network and Information Security (ENISA). European Union. [Online]. Available: https://www.enisa.europa.eu [Accessed May 26, 2018].

[76] European Union Agency for Network and Information Security (ENISA), "The cost of incidents affecting Critical Information Infrastructures," *ENISA Publications*, Aug. 2016.

[77] C. Alcaraz and J. López, "Analysis of requirements for critical control systems," *International Journal of Critical Infrastructure Protection*, vol. 5, no. 3-4, pp. 137–145, Dec. 2012.

[78] S. Karnouskos and A. W. Colombo, "Architecting the next generation of service-based SCADA/DCS system of systems," in *37th Annual Conference of the IEEE Industrial Electronics Society (IECON 2011)*, Melbourne, Australia, Nov. 7–10, 2011, pp. 359–364.

[79] S. M. Rinaldi, J. P. Peerenboom, and T. K. Kelly, "Identifying, understanding, and analyzing critical infrastructure interdependencies," *IEEE Control Systems*, vol. 21, no. 6, pp. 11–25, Dec. 2001.

[80] N. Polemi and P. Kotzanikolaou, "Medusa: A Supply Chain Risk Assessment Methodology," in *4th Cyber Security and Privacy Innovation Forum*, Brussels, Belgium, Apr. 28–29, 2015, pp. 79–90.

[81] Terrorism & other Security-related Risks (CIPS). European Commission. [Online]. Available: https://ec.europa.eu/home-affairs/financing/fundings/security-and-safeguarding-liberties/terrorism-and-other-risks [Accessed Apr. 29, 2018].

[82] MITIGATE Project. [Online]. Available: https://www.mitigateproject.eu [Accessed Apr. 29, 2018].

[83] S. Papastergiou and N. Polemi, "MITIGATE: A Dynamic Supply Chain Cyber Risk Assessment Methodology," in *World Conference on Smart Trends in Systems, Security and Sustainability (WS4)*, London, United Kingdom, Oct. 30–31, 2018, pp. 1–9.

[84] SAURON Project. [Online]. Available: https://www.sauronproject.eu [Accessed Apr. 23, 2018].

[85] Horizon 2020 (H2020). European Commission. [Online]. Available: https://ec.europa.eu/programmes/horizon2020 [Accessed Apr. 29, 2018].

[86] N. Polemi and S. Papastergiou, "Assessing the Risk of Ports and Their Supply Chains: The CYSM, MEDUSA, and MITIGATE Approaches," in *Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense*, E. Carayannis, D. Campbell, and M. Efthymiopoulos, Eds. Cham: Springer International Publishing, 2018, ch. 47, pp. 1011–1038.

[87] R. J. Robles *et al.*, "Common Threats and Vulnerabilities of Critical Infrastructures," *International Journal of Control and Automation*, vol. 1, no. 1, pp. 17–22, 2008.

[88] U. Franke and J. Brynielsson, "Cyber situational awareness – A systematic review of the literature," *Computers & Security*, vol. 46, pp. 18–31, Oct. 2014.

[89] PANOPTESEC Project. [Online]. Available: http://www.panoptesec.eu [Accessed Dec. 20, 2018].

[90] 7th Framework Programme (FP7). European Commission. [Online]. Available: https://ec.europa.eu/research/fp7 [Accessed Dec. 19, 2018].

[91] J. H. Scherrer and W. C. Grund, "A Cyberspace Command And Control Model," *The Maxwell Papers*, no. 47, pp. 1–66, Aug. 2009.

[92] P. Barford *et al.*, "Cyber SA: Situational Awareness for Cyber Defense," in *Cyber Situational Awareness*, ser. Advances in Information Security, S. Jajodia, P. Liu, V. Swarup, and C. Wang, Eds. Boston: Springer, 2010, vol. 46, ch. 1, pp. 3–13.

[93] S. Zonouz, R. Berthier, and N. Arhami, "Towards incorporating human intelligence into online security solutions," in *IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W)*, Boston, United States, Jun. 25–28, 2012, pp. 1–2.

[94] C. Alcaraz and J. López, "Wide-Area Situational Awareness for Critical Infrastructure Protection," *Computer*, vol. 46, no. 4, pp. 30–37, Apr. 2013.

[95] E. D. Matthews, H. J. Arata III, and B. L. Hale, "Cyber Situational Awareness," *The Cyber Defense Review*, vol. 1, no. 1, pp. 35–45, Spring 2016.

[96] P. Salmon, N. Stanton, G. Walker, and D. Green, "Situation awareness measurement: A review of applicability for C4i environments," *Applied Ergonomics*, vol. 37, no. 2, pp. 225–238, Mar. 2006.

[97] R. M. Taylor, "Situational Awareness Rating Technique (SART): The development of a tool for aircrew systems design," in *Proceedings of the AGARD AMP Symposium on Situational Awareness in Aerospace Operations*, no. 478, Copenhagen, Denmark, Oct. 2–6, 1989, pp. 1–17.

[98] G. P. Tadda and J. S. Salerno, "Overview of Cyber Situation Awareness," in *Cyber Situational Awareness*, ser. Advances in Information Security, S. Jajodia, P. Liu, V. Swarup, and C. Wang, Eds. Boston: Springer, 2010, vol. 46, ch. 2, pp. 15–35.

[99] V. Mavroeidis and S. Bromander, "Cyber Threat Intelligence Model: An Evaluation of Taxonomies, Sharing Standards, and Ontologies within Cyber Threat Intelligence," in *2017 European Intelligence and Security Informatics Conference (EISIC)*, Athens, Greece, Sep. 11–13, 2017, pp. 91–98.

[100] MITRE. The MITRE Corporation. [Online]. Available: https://www.mitre.org [Accessed May 13, 2018].

[101] National Institute of Standards and Technology (NIST). U.S. Department of Commerce. [Online]. Available: https://www.nist.gov [Accessed May 13, 2018].

[102] Intel Corporation, "Threat Agent Library Helps Identify Information Security Risks," *Intel Information Technology White Paper*, Sep. 2007.

[103] Intel. Intel Corporation. [Online]. Available: https://www.intel.com [Accessed May 13, 2018].

[104] National Vulnerability Database (NVD). National Institute of Standards and Technology (NIST). [Online]. Available: https://nvd.nist.gov [Accessed May 13, 2018].

[105] Common Vulnerabilities and Exposures (CVE). The MITRE Corporation. [Online]. Available: https://cve.mitre.org [Accessed May 13, 2018].

[106] Common Platform Enumeration (CPE). The MITRE Corporation. [Online]. Available: http://cpe.mitre.org [Accessed May 13, 2018].

[107] Common Weakness Enumeration (CWE). The MITRE Corporation. [Online]. Available: https://cwe.mitre.org [Accessed May 13, 2018].

[108] Common Attack Pattern Enumeration and Classification (CAPEC). The MITRE Corporation. [Online]. Available: https://capec.mitre.org [Accessed May 13, 2018].

[109] Adversarial Tactics, Techniques & Common Knowledge (ATT&CK). The MITRE Corporation. [Online]. Available: https://attack.mitre.org [Accessed May 13, 2018].

[110] NVD Common Vulnerability Scoring System (CVSS). National Institute of Standards and Technology (NIST). [Online]. Available: https://nvd.nist.gov/vuln-metrics/cvss [Accessed May 13, 2018].

[111] Common Weakness Scoring System (CWSS). The MITRE Corporation. [Online]. Available: https://cwe.mitre.org/cwss/cwss_v1.0.1.html [Accessed May 13, 2018].

[112] Structured Threat Information Expression (STIX). The MITRE Corporation. [Online]. Available: https://stixproject.github.io [Accessed Apr. 23, 2018].

[113] C. Sauerwein, C. Sillaber, A. Mussmann, and R. Breu, "Threat Intelligence Sharing Platforms: An Exploratory Study of Software Vendors and Research Perspectives," in *13th International Conference on Wirtschaftsinformatik*, St. Gallen, Switzerland, Feb. 12–15, 2017, pp. 837–851.

[114] Malware Attribute Enumeration and Characterization (MAEC). The MITRE Corporation. [Online]. Available: https://maecproject.github.io/ [Accessed May 13, 2018].

[115] W. Gibb and D. Kerr. (2013, Oct. 1) OpenIOC: Back to the Basics. [Online]. Available: https://www.fireeye.com/blog/threat-research/2013/10/openioc-basics.html [Accessed May 13, 2018].

[116] AlienVault Open Threat Exchange (OTX). AlienVault, Inc. [Online]. Available: https://www.alienvault.com/open-threat-exchange [Accessed May 13, 2018].

[117] Security Content Automation Protocol (SCAP). National Institute of Standards and Technology (NIST). [Online]. Available: https://csrc.nist.gov/projects/security-content-automation-protocol [Accessed Apr. 23, 2018].

[118] Trusted Automated eXchange of Indicator Information (TAXII). The MITRE Corporation. [Online]. Available: https://taxiiproject.github.io [Accessed May 13, 2018].

[119] M. Varga, C. Winkelholz, and S. Träber-Burdin, "Cyber Situation Awareness," *Cyber Security Science and Engineering (STO-EN-IST-143)*, pp. 1–18, Apr. 2016.

[120] M. Tyworth, N. A. Giacobe, V. Mancuso, and C. Dancy, "The distributed nature of cyber situation awareness," in *2012 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA)*, New Orleans, United States, Mar. 6–8, 2012, pp. 174–178.

[121] A. Rajhans *et al.*, "An Architectural Approach to the Design and Analysis of Cyber-Physical Systems," in *Proceedings of the 3rd International Workshop on Multi-Paradigm Modeling (MPM)*, vol. 21, Denver, United States, Oct. 6, 2009, pp. 1–10.

[122] R. Baheti and H. Gill, "Cyber-physical Systems," *The Impact of Control Technology*, pp. 161–166, Feb. 2011.

[123] I. Lendak *et al.*, "Client Side Internet Technologies in Critical Infrastructure Systems," *International Journal of Computers Communications & Control*, vol. 7, no. 5, pp. 879–891, Dec. 2012.

[124] Google Web Toolkit. Google LLC. [Online]. Available: http://www.gwtproject.org [Accessed May 14, 2018].

[125] jQuery. The jQuery Foundation. [Online]. Available: http://jquery.com [Accessed May 14, 2018].

[126] Flex. Adobe, Inc. [Online]. Available: https://www.adobe.com/products/flex.html [Accessed May 14, 2018].

[127] Microsoft Silverlight. Microsoft Corporation. [Online]. Available: https://www.microsoft.com/silverlight [Accessed May 14, 2018].

[128] S. Lu and M. M. Kokar, "A Situation Assessment Framework for Cyber Security Information Relevance Reasoning," in *2015 18th International Conference on Information Fusion*, Washington D.C., United States, Jul. 6–9, 2015, pp. 1459–1466.

[129] E. Gelenbe, G. Görbil, and F.-J. Wu, "Emergency Cyber-Physical-Human Systems," in *2012 21st International Conference on Computer Communications and Networks (ICCCN)*, Munich, Germany, Jul. 2012, pp. 1–7.

[130] D. L. Hall, M. D. McNeese, D. B. Hellar, B. J. Panulla, and W. Shumaker, "A Cyber Infrastructure for Evaluating the Performance of Human Centered Fusion," in *2009 12th International Conference on Information Fusion*, Seattle, United States, Jul. 6–9, 2009, pp. 1257–1264.

[131] G. Klein, C. Ruckert, M. Kleiber, M. Jahnke, and J. Toelle, "Towards a Model-Based Cyber Defense Situational Awareness Visualization Environment," in *Proceedings of the RTO Workshop "Visualising Networks: Coping with Chance and Uncertainty" (RTO-MP-IST-093)*, Rome, New York, United States, Oct. 19–21, 2010, pp. 1–11.

[132] Cybersecurity Solutions. Defense Information Systems Agency (DISA). [Online]. Available: https://www.disa.mil/Cybersecurity [Accessed Apr. 25, 2018].

[133] E. M. Hutchins, M. J. Cloppert, and R. M. Amin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," in *Proceedings of the 6th International Conference on Information Warfare and Security 2011 (ICIW)*, Washington D.C., United States, Mar. 17–18, 2011, pp. 1–12.

[134] T. Yadav and A. M. Rao, "Technical Aspects of Cyber Kill Chain," in *Third International Symposium on Security in Computing and Communication (SSCC)*, Kochi, India, Aug. 10–13, 2015, pp. 438–452.

[135] The MITRE Corporation, "Standardizing cyber threat intelligence information with the Structured Threat Information eXpression (STIX™)," *MITRE Technical Papers*, Jan. 2012.

[136] V. Agham, "Unified Threat Management," *International Research Journal of Engineering and Technology*, vol. 3, no. 4, pp. 32–36, Apr. 2016.

[137] P. Rubens. (2017, Jun. 5) SIEM Guide: A Comprehensive View of Security Information and Event Management Tools. [Online]. Available: https://www.esecurityplanet.com/network-security/security-information-event-management-siem.html [Accessed Jul. 5, 2018].

[138] G. Suárez-Tangil, E. Palomar, A. Ribagorda, and I. Sanz, "Providing SIEM systems with self-adaptation," *Information Fusion*, vol. 21, pp. 145–158, Jan. 2015.

[139] J. D. Pedroza Arango, "Implementación de un Gestor de Seguridad de la Información y Gestión de Eventos (SIEM)," Degree's project, Universidad de San Buenaventura, Medellín, Colombia, 2016.

[140] S. Dorigo, "Security Information and Event Management," Master's thesis, Radboud University Nijmegen, Nijmegen, Netherlands, Aug. 2012.

[141] Gartner, Inc., "Magic Quadrant for Security Information and Event Management," *Gartner Group Research Note*, Dec. 2017.

[142] Best SIEM Solutions & Products. IT Central Station. [Online]. Available: https://www.itcentralstation.com/categories/security-information-and-event-management-siem [Accessed Jun. 6, 2018].

[143] D. Robb. (2017, Jun. 5) Top 10 SIEM Products. [Online]. Available: https://www.esecurityplanet.com/products/top-siem-products.html [Accessed Jun. 6, 2018].

[144] S. Lawton. (2015, Feb. 26) A Guide to Security Information and Event Management. [Online]. Available: http://www.tomsitpro.com/articles/siem-solutions-guide,2-864-2.html [Accessed Jun. 6, 2018].

[145] AlienVault Unified Security Management (USM). AlienVault, Inc. [Online]. Available: https://www.alienvault.com/products/usm-anywhere [Accessed Jul. 5, 2018].

[146] AlienVault Open Source Security Information Management (OSSIM). AlienVault, Inc. [Online]. Available: https://www.alienvault.com/products/ossim [Accessed Apr. 23, 2018].

[147] ArcSight Express. Micro Focus. [Online]. Available: https://software.microfocus.com/en-us/products/arcsight-express-siem-appliance/overview [Accessed Jul. 5, 2018].

[148] ArcSight Enterprise Security Manager (ESM). Micro Focus. [Online]. Available: https://software.microfocus.com/en-us/products/siem-security-information-event-management/overview [Accessed Jul. 5, 2018].

[149] IBM QRadar SIEM. IBM. [Online]. Available: https://www.ibm.com/us-en/marketplace/ibm-qradar-siem [Accessed Jul. 5, 2018].

[150] Security Information and Event Management (SIEM). LogRhythm, Inc. [Online]. Available: https://logrhythm.com/solutions/security/siem [Accessed Jul. 5, 2018].

[151] Splunk Enterprise. Splunk, Inc. [Online]. Available: https://www.splunk.com/en_us/software/splunk-enterprise.html [Accessed Jul. 5, 2018].

[152] Splunk Enterprise Security (ES). Splunk, Inc. [Online]. Available: https://www.splunk.com/en_us/software/enterprise-security.html [Accessed Jul. 5, 2018].

[153] Splunk User Behavior Analytics (UBA). Splunk, Inc. [Online]. Available: https://www.splunk.com/en_us/software/user-behavior-analytics.html [Accessed Jul. 5, 2018].

[154] McAfee Enterprise Security Manager (ESM). McAfee LLC. [Online]. Available: https://www.mcafee.com/enterprise/en-us/products/enterprise-security-manager.html [Accessed Jul. 5, 2018].

[155] NetWitness Platform. RSA Security LLC. [Online]. Available: https://community.rsa.com/community/products/netwitness [Accessed Jul. 5, 2018].

[156] Malware Information Sharing Platform and Threat Sharing (MISP). MISP. [Online]. Available: http://www.misp-project.org [Accessed Apr. 23, 2018].

[157] Request Tracker for Incident Response (RTIR). Best Practical Solutions LLC. [Online]. Available: https://bestpractical.com/rtir [Accessed Apr. 23, 2018].

[158] Request Tracker (RT). Best Practical Solutions LLC. [Online]. Available: https://bestpractical.com/request-tracker [Accessed Jul. 5, 2018].

[159] Wireshark. Wireshark Foundation. [Online]. Available: https://www.wireshark.org [Accessed Jul. 5, 2018].

[160] Ettercap. Ettercap Project. [Online]. Available: http://www.ettercap-project.org [Accessed Jul. 5, 2018].

[161] OpenVAS. OpenVAS. [Online]. Available: http://www.openvas.org [Accessed Jul. 5, 2018].

[162] Nexpose. Rapid7. [Online]. Available: https://www.rapid7.com/products/nexpose [Accessed Jul. 5, 2018].

[163] Snort. Cisco Systems. [Online]. Available: https://www.snort.org [Accessed Jul. 5, 2018].

[164] Suricata. Open Information Security Foundation (OISF). [Online]. Available: https://suricata-ids.org [Accessed Jul. 5, 2018].

[165] Metasploit. Rapid7. [Online]. Available: https://www.rapid7.com/products/metasploit [Accessed Jul. 5, 2018].

[166] Kali Linux Distribution. Kali Linux. [Online]. Available: https://www.kali.org [Accessed Apr. 23, 2018].

[167] Listado Unificado de Coordinación de Incidentes y Amenazas (LUCIA). Centro Criptológico Nacional (CCN-CERT). [Online]. Available: https://www.ccn-cert.cni.es/gestion-de-incidentes/lucia.html [Accessed Oct. 28, 2018].

[168] Centro de Análisis de Registros y Minería de Eventos (CARMEN). Centro Criptológico Nacional (CCN-CERT). [Online]. Available: https://www.ccn-cert.cni.es/soluciones-seguridad/carmen.html [Accessed Jul. 5, 2018].

[169] Gestión de Logs para Respuesta a Incidentes y Amenazas (GLORIA). Centro Criptológico Nacional (CCN-CERT). [Online]. Available: https://www.ccn-cert.cni.es/soluciones-seguridad/gloria.html [Accessed Jul. 5, 2018].

[170] Procedimiento Informático-Lógico para el Análisis de Riesgos (PILAR). Centro Criptológico Nacional (CCN-CERT). [Online]. Available: https://www.ccn-cert.cni.es/soluciones-seguridad/ear-pilar/pilar.html [Accessed Jul. 5, 2018].

[171] Emas IT. S2 Grupo. [Online]. Available: https://s2grupo.es/es/emas-it [Accessed Jul. 5, 2018].

[172] J. Han, M. Kamber, and J. Pei, *Data Mining: Concepts and Techniques*, 3rd ed. San Francisco: Morgan Kaufmann Publishers, 2011.

[173] C. M. Bishop, *Pattern Recognition and Machine Learning*, 1st ed. New York: Springer, 2006.

[174] H. A. Edelstein, *Introduction to Data Mining and Knowledge Discovery*, 3rd ed. Potomac: Two Crows Corporation, 2005.

[175] N. Rikhi, "Data Mining and Knowledge Discovery in Database," *International Journal of Engineering Trends and Technology*, vol. 23, no. 2, pp. 64–70, May 2015.

[176] T. M. Mitchell, *Machine Learning*, 1st ed. New York: McGraw-Hill, 1997.

[177] The R Project for Statistical Computing. The R Foundation. [Online]. Available: https://www.r-project.org [Accessed Apr. 23, 2018].

[178] Python. Python Software Foundation. [Online]. Available: https://www.python.org [Accessed Jul. 24, 2018].

[179] MATLAB. The MathWorks, Inc. [Online]. Available: https://www.mathworks.com/products/matlab.html [Accessed Jul. 24, 2018].

[180] RapidMiner. RapidMiner, Inc. [Online]. Available: https://rapidminer.com [Accessed Apr. 23, 2018].

[181] IBM SPSS Statistics. IBM. [Online]. Available: https://www.ibm.com/products/spss-statistics [Accessed Apr. 23, 2018].

[182] TIBCO Statistica. TIBCO Software, Inc. [Online]. Available: https://www.tibco.com/products/tibco-statistica [Accessed Jul. 24, 2018].

[183] Mathematica. Wolfram. [Online]. Available: https://www.wolfram.com/mathematica [Accessed Jul. 24, 2018].

[184] AdvancedMiner. Algolytics. [Online]. Available: http://algolytics.com/products/advancedminer [Accessed Jul. 24, 2018].

[185] Palantir. Palantir Technologies. [Online]. Available: https://www.palantir.com [Accessed Jul. 24, 2018].

[186] Computational Analysis of Social and Organizational Systems (CASOS). CASOS. [Online]. Available: http://www.casos.cs.cmu.edu [Accessed Jul. 24, 2018].

[187] Sentinel Visualizer. FMS Advanced Systems Group. [Online]. Available: http://www.fmsasg.com [Accessed Jul. 24, 2018].

[188] IBM i2 Analyst's Notebook. IBM. [Online]. Available: https://www.ibm.com/us-en/marketplace/analysts-notebook [Accessed Apr. 23, 2018].

[189] Threat and Risk Management. European Union Agency for Network and Information Security (ENISA). [Online]. Available: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/glossary [Accessed Jul. 24, 2018].

[190] Risk Management. The MITRE Corporation. [Online]. Available: https://www.mitre.org/publications/systems-engineering-guide/acquisition-systems-engineering/risk-management [Accessed Jul. 24, 2018].

[191] P. R. Garvey, *Analytical Methods for Risk Management: A Systems Engineering Perspective*. Chapman and Hall/CRC Press, 2008.

[192] *Risk management – Principles and guidelines*, International Organization for Standardization (ISO), ISO 31 000:2009, Nov. 2009.

[193] A. Syalim, Y. Hori, and K. Sakurai, "Comparison of Risk Analysis Methods: Mehari, Magerit, NIST800-30 and Microsoft's Security Management Guide," in *2009 International Conference on Availability, Reliability and Security (ARES)*, Fukuoka, Japan, Mar. 16–19, 2009, pp. 726–731.

[194] *Méthode Harmonisée d'Analyse des Risques*, Club de la Sécurité des Systèmes d'Information Français (CLUSIF), MEHARI, 1996.

[195] Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT). Ministerio de Hacienda y Administraciones Públicas. [Online]. Available: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html [Accessed Jul. 24, 2018].

[196] *Risk Management Guide for Information Technology Systems*, National Institute of Standards and Technology (NIST), SP 800-30, Jul. 2002.

[197] *Security Risk Management Guide*, Microsoft Corporation, SRMG v1.2, Oct. 2004.

[198] *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*, Ministerio de Hacienda y Administraciones Públicas, MAGERIT Versión 3, Oct. 2012.

[199] F. Zhou, R. Shi, Y. Zhao, Y. Huang, and X. Liang, "NetSecRadar: A Visualization System for Network Security Situational Awareness," in

Proceedings of the 5th International Symposium on Cyberspace Safety and Security (CSS), Zhangjiajie, China, Nov. 13–15, 2013, pp. 403–416.

[200] G.-D. Sun, Y.-C. Wu, R.-H. Liang, and S.-X. Liu, "A Survey of Visual Analytics Techniques and Applications: State-of-the-Art Research and Future Challenges," *Journal of Computer Science and Technology*, vol. 28, no. 5, pp. 852–867, Sep. 2013.

[201] T. Schreck and D. Keim, "Visual Analysis of Social Media Data," *Comuputer*, vol. 46, no. 5, pp. 68–75, May 2013.

[202] E. Bertini and D. Lalanne, "Investigating and reflecting on the integration of automatic data analysis and visualization in knowledge discovery," *ACM SIGKDD Explorations Newsletter*, vol. 11, no. 2, pp. 9–18, May 2010.

[203] IEEE Visualization Conference (VIS 2018). [Online]. Available: http://ieeevis.org/year/2018/welcome [Accessed Jul. 6, 2018].

[204] IEEE Conference on Visual Analytics Science and Technology (VAST 2018). IEEE Visualization Conference (IEEE VIS). [Online]. Available: http://ieeevis.org/year/2018/info/call-participation/vast-paper-types [Accessed Jul. 6, 2018].

[205] IEEE Information Visualization Conference (InfoVis 2018). IEEE Visualization Conference (IEEE VIS). [Online]. Available: http://ieeevis.org/year/2018/info/call-participation/infovis-paper-types [Accessed Jul. 6, 2018].

[206] IEEE Scientific Visualization Conference (SciVis 2018). IEEE Visualization Conference (IEEE VIS). [Online]. Available: http://ieeevis.org/year/2018/info/call-participation/scivis-paper-types [Accessed Jul. 6, 2018].

[207] IEEE Symposium on Visualization for Cyber Security (VizSec). [Online]. Available: http://vizsec.org [Accessed Jul. 6, 2018].

[208] Luciad Company. [Online]. Available: http://www.luciad.com [Accessed Apr. 23, 2018].

[209] LuciadLightspeed. Luciad Company. [Online]. Available: http://www.luciad.com/solutions/luciadlightspeed [Accessed Jul. 6, 2018].

[210] LuciadRIA. Luciad Company. [Online]. Available: http://www.luciad.com/solutions/luciadria [Accessed Jul. 6, 2018].

[211] LuciadFusion. Luciad Company. [Online]. Available: http://www.luciad.com/solutions/luciadfusion [Accessed Jul. 6, 2018].

[212] LuciadMobile. Luciad Company. [Online]. Available: http://www.luciad.com/solutions/luciadmobile [Accessed Jul. 6, 2018].

[213] ArcGIS. ESRI. [Online]. Available: https://www.esri.com/en-us/arcgis/about-arcgis/overview [Accessed Jul. 6, 2018].

[214] Carmenta. Carmenta Group. [Online]. Available: https://www.carmenta.com [Accessed Jul. 6, 2018].

[215] Google Maps. Google LLC. [Online]. Available: https://www.google.com/maps [Accessed Jul. 6, 2018].

[216] Bing Maps. Microsoft Corporation. [Online]. Available: https://www.bing.com/maps [Accessed Jul. 6, 2018].

[217] OpenStreetMap. OpenStreetMap Foundation. [Online]. Available: https://www.openstreetmap.org [Accessed Jul. 6, 2018].

[218] Cesium. Cesium Consortium. [Online]. Available: https://cesium.com [Accessed Apr. 23, 2018].

[219] OpenLayers. Open Source Geospatial Foundation (OSGeo). [Online]. Available: https://openlayers.org [Accessed Jul. 6, 2018].

[220] Carto. CartoDB, Inc. [Online]. Available: https://carto.com [Accessed Jul. 6, 2018].

[221] R. Marty, *Applied Security Visualization*. Addison-Wesley Professional, 2009.

[222] F. Fischer and D. A. Keim, "VACS: Visual Analytics Suite for Cyber Security - Visual Exploration of Cyber Security Datasets," in *2013 IEEE Visual Analytics Science and Technology Challenge (VAST)*, Atlanta, United States, Oct. 13–18, 2013, pp. 1–2.

[223] M. Angelini, N. Prigent, and G. Santucci, "PERCIVAL: proactive and reactive attack and response assessment for cyber incidents using visual analytics," in *2015 IEEE Symposium on Visualization for Cyber Security (VizSec)*, Chicago, United States, Oct. 25, 2015, pp. 1–8.

[224] B. Balakrishnan, "Security Data Visualization," *The SANS Institute - InfoSec Reading Room*, pp. 1–51, Oct. 2015.

[225] Microsoft Chart Controls. Microsoft Corporation. [Online]. Available: https://www.microsoft.com/en-us/download/details.aspx?id=14422 [Accessed Jul. 23, 2018].

[226] Chart.js. [Online]. Available: https://www.chartjs.org [Accessed Jul. 23, 2018].

[227] JpGraph. Asial Corporation. [Online]. Available: https://jpgraph.net [Accessed Jul. 23, 2018].

[228] Three.js. [Online]. Available: https://threejs.org [Accessed Jul. 23, 2018].

[229] JavaScript InfoVis Toolkit. SenchaLabs. [Online]. Available: https://philogb.github.io/jit [Accessed Jul. 23, 2018].

[230] Data-Driven Documents. [Online]. Available: https://d3js.org [Accessed Jul. 23, 2018].

[231] O.-H. Kwon, C. Muelder, K. Lee, and K.-L. Ma, "Spherical Layout and Rendering Methods for Immersive Graph Visualization," in *2015 IEEE Pacific Visualization Symposium (PacificVis)*, Hangzhou, China, Apr. 14–17, 2015, pp. 63–67.

[232] S. Royston, C. DeFanti, and K. Perlin, "A Collaborative Untethered Virtual Reality Environment for Interactive Social Network Visualization," *eprint arXiv:1604.08239*, Apr. 2016.

[233] A. Kirk. Visualising Data. [Online]. Available: http://www.visualisingdata.com [Accessed Jul. 23, 2018].

[234] M. Lima. Visual Complexity. [Online]. Available: http://www.visualcomplexity.com [Accessed Jul. 23, 2018].

[235] S. Saleem. GraphOverflow. [Online]. Available: http://graphoverflow.com [Accessed Jul. 23, 2018].

[236] Chrome Experiments. Google LLC. [Online]. Available: https://www.chromeexperiments.com [Accessed Jul. 23, 2018].

[237] Tableau. Tableau Software. [Online]. Available: https://www.tableau.com [Accessed Jul. 23, 2018].

[238] Datawrapper. Datawrapper GmbH. [Online]. Available: https://www.datawrapper.de [Accessed Jul. 23, 2018].

[239] Infogram. Prezi, Inc. [Online]. Available: https://infogram.com [Accessed Jul. 23, 2018].

[240] M. Hyland and J. Flood. (2017, Jul. 3) The Emergence of Virtual Reality and Augmented Reality in the Security Operations Center. [Online]. Available: https://securityintelligence.com/the-emergence-of-virtual-reality-and-augmented-reality-in-the-security-operations-center [Accessed Jul. 23, 2018].

[241] W. Greenwald. (2018, Jun. 25) The Best VR (Virtual Reality) Headsets of 2018. [Online]. Available: https://www.pcmag.com/article/342537/the-best-virtual-reality-vr-headsets [Accessed Jul. 23, 2018].

[242] Oculus Rift. Oculus VR. [Online]. Available: https://www.oculus.com/rift [Accessed Apr. 26, 2018].

[243] Samsung Gear VR. Samsung. [Online]. Available: https://www.samsung.com/us/mobile/virtual-reality/gear-vr [Accessed Jul. 23, 2018].

[244] VIVE Virtual Reality System. HTC Corporation. [Online]. Available: https://www.vive.com/us/product/vive-virtual-reality-system [Accessed Jul. 23, 2018].

[245] Daydream View. Google LLC. [Online]. Available: https://vr.google.com/daydream/smartphonevr [Accessed Jul. 23, 2018].

[246] Oculus Go. Oculus VR. [Online]. Available: https://www.oculus.com/go [Accessed Jul. 23, 2018].

[247] Mirage Solo. Lenovo. [Online]. Available: https://www.lenovo.com/us/en/virtual-reality-and-smart-devices/virtual-and-augmented-reality/lenovo-mirage-solo/Mirage-Solo/p/ZZIRZRHVR01 [Accessed Jul. 23, 2018].

[248] HMD Odissey - Windows Mixed Reality. Samsung. [Online]. Available: https://www.samsung.com/us/computing/hmd/windows-mixed-reality/xe800zaa-hc1us-xe800zaa-hc1us [Accessed Jul. 23, 2018].

[249] Windows Mixed Reality. Microsoft Corporation. [Online]. Available: https://www.microsoft.com/en-us/windows/windows-mixed-reality [Accessed Jul. 23, 2018].

[250] Cesium-VR Plugin. [Online]. Available: https://github.com/NICTA/cesium-vr [Accessed Jul. 23, 2018].

[251] Cesium-Leap Plugin. [Online]. Available: https://github.com/Aviture/cesium-leap [Accessed Jul. 23, 2018].

[252] Oculus VR. [Online]. Available: https://www.oculus.com [Accessed Oct. 2, 2018].

[253] Unity. [Online]. Available: https://unity3d.com [Accessed Apr. 26, 2018].

[254] AggreGate SCADA/HMI. Tibbo Systems. [Online]. Available: http://aggregate.tibbo.com/solutions/industrial-automation/scada-hmi.html [Accessed Oct. 27, 2018].

[255] Graphene. Assac Networks. [Online]. Available: https://assacnetworks.com/scada-cyber-security [Accessed Oct. 27, 2018].

[256] M. Iturbe, I. Garitano, U. Zurutuza, and R. Uribeetxeberria, "Towards Large-Scale, Heterogeneous Anomaly Detection Systems in Industrial Networks: A Survey of Current Trends," *Security and Communication Networks*, vol. 2017, pp. 1–17, Nov. 2017.

[257] C. Wagner, A. Dulaunoy, G. Wagener, and A. Iklody, "MISP: The Design and Implementation of a Collaborative Threat Intelligence Sharing Platform," in *Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security (WISCS)*, Vienna, Austria, Oct. 24, 2016, pp. 49–56.

[258] AlienVault APIs. AlienVault, Inc. [Online]. Available: https://www.alienvault.com/documentation/api/av-apis.htm [Accessed Oct. 17, 2018].

[259] B. Costa, P. F. Pires, F. C. Delicato, and P. Merson, "Evaluating a Representational State Transfer (REST) Architecture: What is the Impact of REST in My Architecture?" in *2014 IEEE/IFIP Conference on Software Architecture*, Sydney, Australia, Apr. 7–11, 2014, pp. 105–114.

[260] PyMISP - Python Library to access MISP. Malware Information Sharing Platform and Threat Sharing (MISP). [Online]. Available: https://github.com/MISP/PyMISP [Accessed Oct. 27, 2018].

[261] RT Extension - API REST2. Best Practical Solutions LLC. [Online]. Available: https://github.com/bestpractical/rt-extension-rest2 [Accessed Oct. 27, 2018].

[262] *NATO Vector Graphics (NVG)*, NATO Allied Command Transformation (ACT), NVG Version 1.5:2010, 2008.

[263] Scalable Vector Graphics (SVG). World Wide Web Consortium (W3C). [Online]. Available: https://www.w3.org/Graphics/SVG [Accessed Oct. 27, 2018].

[264] S. Dustdar and W. Schreiner, "A Survey on Web Services Composition," *International Journal of Web and Grid Services*, vol. 1, no. 1, pp. 1–30, Aug. 2005.

[265] J. S. Bowman, S. L. Emerson, and M. Darnovsky, *The Practical SQL Handbook: Using Structured Query Language*, 3rd ed. Addison-Wesley Longman Publishing Co., Inc., 1996.

[266] SQL Server. Microsoft Corporation. [Online]. Available: https://www.microsoft.com/en-us/sql-server/sql-server-2017 [Accessed Oct. 27, 2018].

[267] Oracle Database. Oracle Corporation. [Online]. Available: https://www.oracle.com/database [Accessed Oct. 27, 2018].

[268] MySQL Database. Oracle Corporation. [Online]. Available: https://www.mysql.com/products/enterprise/database [Accessed Oct. 27, 2018].

[269] F. Gessert and N. Ritter, "Scalable data management: NoSQL data stores in research and practice," in *2016 IEEE 32nd International Conference on Data Engineering (ICDE)*, Helsinki, Finland, May 16–20, 2016, pp. 1420–1423.

[270] C. J. M. Tauro, S. Aravindh, and A. B. Shreeharsha, "Comparative Study of the New Generation, Agile, Scalable, High Performance NOSQL Databases," *International Journal of Computer Applications*, vol. 48, no. 20, pp. 1–4, Jun. 2012.

[271] Apache Cassandra. Apache Software Foundation. [Online]. Available: http://cassandra.apache.org [Accessed Apr. 23, 2018].

[272] Apache HBase. Apache Software Foundation. [Online]. Available: https://hbase.apache.org [Accessed Oct. 27, 2018].

[273] MongoDB. MongoDB, Inc. [Online]. Available: https://www.mongodb.com [Accessed Apr. 23, 2018].

[274] C. M. Bishop, *Neural Networks for Pattern Recognition*. New York: Oxford University Press, Inc., 1995.

[275] R. O. Duda, P. E. Hart, and D. G. Stork, *Pattern Classification*, 2nd ed. New York: John Wiley & Sons, Inc., 2004.

[276] Google Places. Google LLC. [Online]. Available: https://cloud.google.com/maps-platform/places [Accessed Sep. 29, 2018].

[277] T. Segaran and J. Hammerbacher, *Beautiful Data: The Stories Behind Elegant Data Solutions*. O'Reilly Media, 2009.

[278] B. Fry, *Visualizing Data: Exploring and Explaining Data with the Processing Environment*. O'Reilly Media, 2008.

[279] S. E. Noel, E. Harley, K. H. Tam, M. Limiero, and M. Share, "CyGraph: Graph-Based Analytics and Visualization for Cybersecurity," in *Cognitive Computing: Theory and Applications*, ser. Handbook of Statistics, V. Gudivada, V. Raghavan, V. Govindaraju, and C. R. Rao, Eds. Elsevier, 2016, vol. 35, ch. 4, pp. 117–167.

[280] Visual Analytics for Command, Control and Interoperability Environments (VACCINE). Purdue University. [Online]. Available: https://www.purdue.edu/discoverypark/vaccine [Accessed Oct. 25, 2018].

[281] .NET. Microsoft Corporation. [Online]. Available: https://www.microsoft.com/NET [Accessed Nov. 4, 2018].

[282] Keyhole Markup Language (KML). Google LLC. [Online]. Available: https://developers.google.com/kml [Accessed Apr. 23, 2018].

[283] NVIDIA GeForce GTX 970. NVIDIA Corporation. [Online]. Available: https://www.geforce.com/hardware/desktop-gpus/geforce-gtx-970 [Accessed Nov. 29, 2018].

[284] Y. Rebahi *et al.*, "Virtual security appliances: the next generation security," in *2015 International Conference on Communications, Management and Telecommunications (ComManTel)*, Da Nang, Vietnam, Dec. 28–30, 2015, pp. 103–110.

[285] VMware ESXi. VMware, Inc. [Online]. Available: https://www.vmware.com/products/esxi-and-esx.html [Accessed Nov. 29, 2018].

[286] VMware vCenter Server. VMware, Inc. [Online]. Available: https://www.vmware.com/products/vcenter-server.html [Accessed Nov. 29, 2018].

[287] Scalable multidimensionAl sitUation awaReness sOlution for protectiNg european ports (SAURON). European Commission. [Online]. Available: https://cordis.europa.eu/project/rcn/210044 [Accessed Nov. 30, 2018].

[288] Fundación Valenciaport. [Online]. Available: http://www.fundacion.valenciaport.com [Accessed Nov. 30, 2018].

[289] Noatum. [Online]. Available: https://www.noatum.com [Accessed Nov. 30, 2018].

[290] Piraeus Port Authority. [Online]. Available: http://www.olp.gr [Accessed Nov. 30, 2018].

[291] Autorità di Sistema Portuale del Mar Tirreno Settentrionale. [Online]. Available: https://www.portialtotirreno.it [Accessed Nov. 30, 2018].

[292] Luka Koper. [Online]. Available: https://www.luka-kp.si [Accessed Nov. 30, 2018].

[293] Universidad Politécnica de Valencia. [Online]. Available: https://www.upv.es [Accessed Nov. 30, 2018].

[294] University of Piraeus. [Online]. Available: http://www.unipi.gr/unipi [Accessed Nov. 30, 2018].

[295] Katholieke Universiteit Leuven. [Online]. Available: https://www.kuleuven.be [Accessed Nov. 30, 2018].

[296] Austrian Institute of Technology. [Online]. Available: https://www.ait.ac.at [Accessed Nov. 30, 2018].

[297] Thales Group. [Online]. Available: https://www.thalesgroup.com [Accessed Nov. 30, 2018].

[298] IDEMIA. [Online]. Available: https://www.morpho.com [Accessed Nov. 30, 2018].

[299] Grupo ETRA. [Online]. Available: http://www.grupoetra.com [Accessed Nov. 30, 2018].

[300] S2 Grupo. [Online]. Available: https://s2grupo.es [Accessed Nov. 30, 2018].

[301] InnovaSec. [Online]. Available: https://www.innovasec.co.uk [Accessed Nov. 30, 2018].

[302] S. Schauer *et al.*, "Conceptual Framework for Hybrid Situational Awareness in Critical Port Infrastructures," in *13th International Conference on Critical Information Infrastructures Security (CRITIS)*, Kaunas, Lithuania, Sep. 24–26, 2018, pp. 191–203.

[303] European Defence Agency (EDA). European Union Council. [Online]. Available: https://www.eda.europa.eu [Accessed Nov. 13, 2018].

[304] NATO Counter-Improvised Explosive Devices Centre of Excellence (C-IED CoE), "Newsletter December 2016," *NATO C-IED CoE Newsletters*, Dec. 2016.

[305] EDA Press Centre. (2016, Nov. 15) EDA to offer new C-IED application for improved situational awareness. Brussels. [Online]. Available: https://www.eda.europa.eu/info-hub/press-centre/latest-news/2016/11/15/eda-to-offer-new-c-ied-application-for-improved-situational-awareness [Accessed Nov. 14, 2018].

[306] Counter-Improvised Explosive Devices Centre of Excellence (C-IED CoE). North Atlantic Treaty Organization (NATO). [Online]. Available: https://ciedcoe.org [Accessed Nov. 13, 2018].

[307] D. Vincen, D. Stampouli, and G. Powell, "Foundations for System Implementation for a Centralised Intelligence Fusion Framework for Emergency Services," in *2009 12th International Conference on Information Fusion*, Seattle, United States, Jul. 6–9, 2009, pp. 1401–1408.

[308] Internet Information Services (IIS). Microsoft Corporation. [Online]. Available: https://www.iis.net [Accessed Nov. 10, 2018].

[309] Angular. [Online]. Available: https://angularjs.org [Accessed Apr. 23, 2018].

[310] Electron. [Online]. Available: https://electronjs.org [Accessed Apr. 23, 2018].

[311] Ionic. [Online]. Available: https://ionicframework.com [Accessed Apr. 23, 2018].

[312] Predictive Analytics. SAP. [Online]. Available: https://www.sap.com/products/predictive-analytics.html [Accessed Apr. 23, 2018].

[313] Elasticsearch. Elasticsearch B.V. [Online]. Available: https://www.elastic.co/products/elasticsearch [Accessed Dec. 22, 2018].

[314] RabbitMQ. Pivotal Software, Inc. [Online]. Available: https://www.rabbitmq.com [Accessed Dec. 22, 2018].

[315] Apache Kafka. Apache Software Foundation. [Online]. Available: https://kafka.apache.org [Accessed Dec. 22, 2018].