

# Índice

Índice de figuras	XIII
Índice de tablas	XV
Acrónimos	XVII
<b>1. Introducción</b>	<b>1</b>
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
<b>2. Estado del arte</b>	<b>11</b>
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. <i>Cyber Situational Awareness</i> . . . . .	32
2.4.1. Marco general . . . . .	32

## ÍNDICE

---

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
<b>3.</b>	<b>Definición de la arquitectura</b>	<b>59</b>
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
<b>4.</b>	<b>Validación de la arquitectura: GESTPIC</b>	<b>81</b>
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
<b>5.</b>	<b>Evaluación del sistema GESTPIC</b>	<b>99</b>
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
<b>6. Validación de la arquitectura: HYBINT</b>	<b>111</b>
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
<b>7. Conclusiones</b>	<b>125</b>
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
<b>Referencias</b>	<b>133</b>