TESIS DOCTORAL

2021

CREACIÓN Y DESPLIEGUE DE ARQUITECTURAS HÍBRIDAS PARA LA MEJORA DE LA CIBERSEGURIDAD EN SISTEMAS DE CONTROL INDUSTRIAL EN INFRAESTRUCTURAS CRÍTICAS

SANTIAGO GONZÁLEZ GONZÁLEZ

PROGRAMA DE DOCTORADO EN INGENIERÍA DE SISTEMAS Y DE CONTROL

DIRECTORES: SEBASTIÁN DORMIDO CANTO/JOSÉ SÁNCHEZ MORENO

UNED Escuela Internacional de Doctorado EIDUNED

TESIS DOCTORAL

Creación y despliegue de arquitecturas híbridas para la mejora de la ciberseguridad en sistemas de control industrial en infraestructuras críticas

Programa Doctorado en Ingeniería de Sistemas y Control

Autor: **D. Santiago González González**

Directores: Dr. D. Sebastián Dormido Canto

Dr. D. José Sánchez Moreno

Octubre 2021


UNED
Escuela
Internacional
de Doctorado
EIDUNED

UNIVERSIDAD DE EDUCACIÓN A DISTANCIA

Escuela Internacional de Doctorado
Departamento de Informática y Automática (DIA)
Escuela Técnica Superior de Ingeniería Informática (ETSI)

Creación y despliegue de arquitecturas híbridas para la mejora de la ciberseguridad en sistemas de control industrial en infraestructuras críticas

Autor de la Tesis Doctoral
D. Santiago González González
Master en Ingeniería de Sistemas y Control por la Universidad de Educación a Distancia

Directores de la Tesis Doctoral
Dr. D. Sebastián Dormido Canto
Catedrático de la Universidad Nacional de Educación a Distancia
Dr. D. José Sánchez Moreno
Catedrático de la Universidad Nacional de Educación a Distancia

Madrid, octubre de 2021

Declaración de autoría

Yo, Santiago González González, declaro que el trabajo llevado a cabo en esta Tesis por título **"Creación y despliegue de arquitecturas híbridas para la mejora de la ciberseguridad en sistemas de control industrial en infraestructuras críticas"**, ha sido realizado por mí y son de mi propiedad. A su vez afirmo que:

- En caso de que alguna parte de esta Tesis haya sido presentada previamente para una licenciatura o cualquier otra titulación en esta Universidad o en cualquier otra institución, ha sido detallado de una manera clara y concisa.
- Cuando se ha consultado el trabajo publicado de otros investigadores, en todo momento han sido debidamente citados y atribuidos.
- Cuando se ha citado el trabajo de otros autores, siempre ha sido indicada la fuente.
- A excepción de estas citas, la autoría de esta Tesis se corresponde con el autor de este trabajo de investigación.
- Han sido reconocidas todas las fuentes de consulta y ayuda como complemento a la presente investigación.
- En los casos en los que la Tesis posee fuentes de apoyo técnico o se ha basado en trabajos realizados por el autor del presente estudio junto con otros, y con el apoyo de material propiedad de otras instituciones, se ha procedido a aclararlo, detallando el trabajo aportado por el resto de personas e instituciones.

El Espinar, octubre de 2021

Firmado: Santiago González González

Firmado digitalmente por GONZALEZ GONZALEZ SANTIAGO - 03465430C el día 29/09/2021 con un certificado emitido por AC FNMT Usuarios

"Prefiero una actitud de humildad que se corresponda con la debilidad de nuestra capacidad intelectual para comprender la naturaleza de nuestro propio ser".

Albert Einstein.

Mención especial

He conocido dos mujeres en el mundo que han marcado a fuego mi destino en la vida y que, sin las cuales, no habría habido posibilidad de encontrar sentido a mi existencia. Una de ellas es mi madre María Victoria, que me dio todo a cambio de nada, y a la que por desgracia no tuve tiempo de corresponderle como se hubiese merecido. Cuanto te echo de menos madre !!!.

Aurora, mi pareja, mi amiga, mi confesora y mi guía, muchas gracias por haber estado ahí desde el principio, desde que me inculcaste y me apoyaste en aquella loca propuesta de que cursara una ingeniería a la vez que trabajaba. Gracias por aguantar toda la soledad que te he causado por mis largos encierros y ausencias. Gracias por darme siempre otros puntos de vista y gracias de nuevo por seguir estando aquí conmigo. Deseo poder dedicarte todo el tiempo de mi vida a seguir agradeciéndote cosas.

Os quiero con todo mi corazón.

Resumen

Los avances en las Tecnologías de la Información (TI) están dotando a los Sistemas de Control Industrial (SCI) de una gran capacidad de interconexión y adaptabilidad. Sin embargo, la utilización de las redes de comunicaciones al uso hace a los SCI altamente vulnerables. En consecuencia, es imprescindible desarrollar metodologías para la identificación y posterior clasificación de los SCI que intervienen en activos desplegados en infraestructuras críticas, con cualquier nivel de complejidad, escalabilidad y heterogeneidad. El Sistema de Infraestructura del Conocimiento para la Experimentación Real mediante Células de Automatización Industrial (SICERCAI), descrito en el presente trabajo, proporciona nuevas capacidades para la investigación, desarrollo, simulación y tentativa de funcionamiento de estos sistemas, así como la capacidad de prever el comportamiento específico en el área de la producción industrial. Los escenarios recreados a través de SICERCAI poseen la capacidad de anticiparse a las nuevas amenazas que afectan a los SCI de las infraestructuras críticas. Utilizando SICERCAI se ha verificado una vulnerabilidad concreta de un controlador lógico programable (Programmable Logic Controller, PLC, por sus siglas en inglés), a través de la ingeniería programada para la gestión de un sistema de control de tráfico de vehículos y peatones. Los resultados obtenidos demuestran la alta dependencia entre las TI y las Tecnologías de la Operación (TO). Y por tanto, la importancia de poder recrear esos entornos críticos como paso previo a su despliegue y puesta en funcionamiento.

Al ser SICERCAI un sistema abierto se puede usar para testear componentes de diferentes fabricantes industriales, aproximándose así a los existentes en la industria de procesos.

Una parte del presente trabajo de investigación, se encuentra publicado en la revista "International Journal of Critical Infrastructure Protection" de la editorial ELSEVIER.
(https://doi.org/10.106/j.ijcip.2020.100355)

Palabras clave:

Ciberseguridad, sistemas de control industrial, infraestructuras críticas, seguridad nacional, ciber-resiliencia, agrupación de tecnologías de la información y tecnologías de la operación, laboratorio de pruebas, alta disponibilidad, dependencias tecnológicas, centro de procesos de datos

Abstract

The advances in Information Technologies (IT) are providing Industrial Control Systems (ICS) with a great capacity for interconnection and adaptability. However, the use of communication networks makes ICS highly vulnerable. Consequently, it is essential to develop methodologies for the identification and subsequent classification of the ICS that intervene in critical infrastructure assets with any level of complexity, scalability and heterogeneity. The System and Infrastructure of Knowledge for Real Experimentation by means of Cells of Industrial Automation (SIKRECIA), described in this work, provides new capabilities for research, development, simulation and testing of the functioning of these systems, and the ability to fore- see the behavior of a specific system in industrial production. The scenarios recreated through SIKRECIA have the ability to anticipate new threats that affect the ICS of critical infrastructures. Using SIKRECIA, a specific vulnerability of a programing logic controller (PLC) has been verified through the engineering programmed for the management of a traffic light control system. The results obtained demonstrate the high dependence between IT and OT (Operation Technologies) systems and therefore the importance of being able to recreate those environments before entering into operation.

As SIKRECIA is an open system, it can be used to test components from different industrial manufacturers, thus approaching those existing in the process industry.

Part of this research work is published in the "International Journal of Critical Infrastructure Protection" published by ELSEVIER.”

(https://doi.org/10.106/j.ijcip.2020.100355)

Keywords:

Cybersecurity, industrial control system, critical infrastructure, national security, cyber resilience, clustering, information technology, operational technology, test bed, high availability, technology units.

Prólogo

Estos últimos cuatro años y medio, para mí personalmente, se han correspondido con una etapa de mi vida cargada de ilusiones, desilusiones, experiencias, y aprendizajes, que me han generado nuevas inquietudes y retos (en lo personal, emocional y lo profesional), que difícilmente sería capaz de detallar meritoriamente en esta sección, dada su extensión.

A lo largo de este documento, he llevado a cabo una síntesis de lo que ha supuesto para mi vida académica, que comencé ya hace mucho tiempo atrás, y que en los últimos 20 años he desarrollado en paralelo junto a mi vida laboral y familiar, siendo el zenit de ese camino, esta Tesis Doctoral.

Quisiera aprovechar la oportunidad en esta sección para detallar cuales fueron algunas de esas intrigas y vivencias que me despertaron las ganas de embarcarme en este duro trabajo llevado a cabo.

Tras varios años en el mundo de la informática, en el cual llevaba poniendo en práctica mis *experimentos*, alentados por mi intriga por saber y conocer, desde que era un pre-adolescente, tuve la suerte de toparme en mi vida académica con uno de mis directores de la Tesis. Sebastián despertó en mí las ganas de saber *"por qué los 0 y los 1, combinados adecuadamente y tratados electrónicamente, componían el alma de los ordenadores"*. Esto para mí resultó mágico a la vez que intrigante.

Varios años después, esta misma persona me ofreció la oportunidad, y sobre todo confió en mí para desarrollar un trabajo fin de máster en Ingeniería de Sistemas y Control, que sería tutorizado junto a Jesús Vega, doctor en ciencias físicas del CIEMAT. ¿Cómo consiguieron mi compromiso incondicional?, simplemente Sebastián Dormido y Jesús Vega, supieron

despertarme ese *gusanillo del saber*, me mostraron el reactor de fusión nuclear que hay en el CIEMAT. Esto combinado con mis ganas, me marcó durante todo el desarrollo del máster.

En esta época, mi perfil laboral, puramente alineado con las Tecnologías de la Información, se presentaba ambicioso como resultado de mi contacto con la protección de infraestructuras críticas. Comienzo, entonces, mi andadura con los sistemas de control y automatismos industriales involucrados en esas infraestructuras. ¿Qué era eso de la ciberseguridad industrial?. Puedo asegurar que cuando empecé mi camino en este área tan específica, me sentía como un predicador sin rumbo en medio del desierto.

Como no podía ser de otra manera, mis ganas de saber me volvieron a provocar para enrolarme en este tema. Como resultado de ello, la investigación plasmada en esta Tesis.

En todo momento he sido alentado y reconocido por mis directores Sebastián y José, los cuales, mediante su apoyo humano, y profesionalidad ofrecida, han hecho que este trabajo resulte para mí, un resumen de un capítulo de mi vida.

Esta Tesis Doctoral me ha proporcionado la capacidad de haber sido capaz de impartir varios talleres prácticos a alumnos de diferentes cursos universitarios, Fuerzas y Cuerpos de Seguridad del Estado, y a empresas del área de la ciberseguridad industrial. A su vez, he tenido el honor de impartir un webinar dentro de la ISA (International Sociaty of Automation), así como haber sido invitado como investigador de un proyecto de exploración de vulnerabilidades en sistemas de control industrial en infraestructuras críticas, en el centro de ciber-excelencia de la OTAN (Tallin-Estonia).

Como no puede ser de otra manera, ya que en paralelo a mis ganas de saber, caminan mis ganas de enseñar lo poquito que sé, he podido disfrutar de varios programas de televisión y programas radiofónicos, en los que he intentado transmitir mi entusiasmo y mis ganas de conocer al resto de personas.

Agradecimientos

Para comenzar quisiera otorgar mi más sincero agradecimiento a mis directores de Tesis Dr. D. Sebastián Dormido Canto y Dr. D. José Sánchez Moreno, por su incondicional e ilimitada ayuda, y apoyo prestado a lo largo de los años para la preparación y desarrollo de este trabajo. Mi realización científica no hubiese culminado en esta Tesis si no hubieran estado ahí desde muchos años atrás, ofreciéndome siempre nuevas vías de motivación e investigación.

Agradezco a mis suegros Juana María y José Luis, su curiosidad y apoyo incondicional por mis trabajos, por mis estudios, y por mi vida en general. Os quiero como si fueseis mis padres.

Agradezco toda comprensión, complicidad y apoyo a mis cuñados y cuñadas, gracias Miguel, Javi, José Luis, Rubén, Sara y María Jesús.

A tod@s mis amig@s, los cuales habéis aguantado mis cambios de humor, muchas veces debidos a estrés producido por el trabajo ingente que ha dado forma a mi Tesis Doctoral. Siempre habéis estado ahí en lo bueno y en lo menos bueno apoyando y animándome en mis decisiones. No os numero por si a caso se me olvida alguien y no quiero correr ese riesgo.

Ana, incondicional y fantástica investigadora y amiga, muchas gracias por cambiar mi forma de hablar referente a mí *"cabezonería"* la cual, gracias a ti he logrado transformarla en *"perseverancia"*. Gracias a esa perseverancia presento mi trabajo en forma de Tesis Doctoral. Un verdadero sueño hecho realidad.

Debo dar las gracias de igual manera, a todas aquellas personas que han compartido conmigo momentos en el trabajo y fuera de él, a los cuales, cuando les explicaba lo que estaba desarrollando no les quedaba muy claro mi investigación, pero apoyaron mis ideas. A ti Alfonso, que estuviste conmigo luchando con esto de “la ciberseguridad industrial” aguantando y compartiendo mis propuestas a veces alocadas, y que, al final creo haber logrado inculcarte y haberte despertado el gusanillo. Gracias amigo!!!.

Para finalizar, pero no por ello menos importante, agradezco a Pilar y a María José, su amistad y ayuda incondicional prestada desde la secretaría de la Universidad.

Índice general

Declaración de autoría I

Mención especial IV

Resumen.....VI

Abstract VIII

Prólogo X

Agradecimientos XV

Índice general XVII

Listas de figuras y tablas XXV

Figuras XXV

Tablas XXXI

Lista de ecuaciones XXXIII

Lista de scripts XXXV

Lista de abreviaturas XXXVI

Capítulo I

1. Prólogo ..... - 1 -

1.1. Tecnologías de la Información y Tecnologías de la Operación..... - 5 -

1.2. Convergencia de las Tecnologías de la Información y las Tecnologías de la Operación..... - 9 -

1.3. Concepto de ciberseguridad en entornos industriales..... - 15 -

1.4. Importancia de la ciberseguridad en entornos industriales ..... - 17 -
1.5. Ciberseguridad y ciber-resiliencia ..... - 21 -
1.5.1. Infraestructuras críticas ..... - 22 -
1.6. Estructura de la Tesis ..... - 25 -
1.7. Resumen ..... - 28 -

Capítulo II

2. Objetivos - 31 -
2.1. Objetivos generales ..... - 31 -
2.2. Objetivos específicos ..... - 32 -
2.3. Importancia de la ciberseguridad en las TO y en las infraestructuras críticas - 34 -
2.4. Motivaciones de la investigación ..... - 36 -
2.5. Clasificación de la hipótesis de partida ..... - 37 -
2.5.1. Adaptabilidad según necesidad ..... - 38 -
2.5.2. Efectividad ..... - 39 -
2.5.3. Estructura ..... - 40 -
2.5.4. Método ..... - 40 -
2.6. Metodología desarrollada en la investigación ..... - 41 -
2.7. Resumen ..... - 43 -

Capítulo III

3. Introducción ..... - 47 -
3.1. Marco metodológico ..... - 48 -
3.2. Marco teórico ..... - 49 -
3.2.1. Madurez de los sistemas ..... - 51 -
3.2.2. Principales marcos de referencia de evaluación de madurez de la ciberseguridad en TO ..... - 54 -
3.2.2.1. Marco de ciberseguridad NIST 1.1 (NIST-CF) ..... - 56 -
3.2.2.2. Modelo de madurez de las capacidades de ciberseguridad C2M2 ..... - 59 -
3.2.3. Alcance de la investigación realizada ..... - 61 -

3.2.4. Partes implicadas en los procesos de la ciberseguridad industrial ..... - 62 -
3.2.4.1.Partes intervinientes de carácter interno ..... - 64 -
3.2.4.2 Partes intervinientes externas ..... - 66 -
3.2.4.3 Partes intervinientes contribuidoras al proceso productivo ..... - 67 -
3.2.5. Exposición de los sistemas industriales en internet ..... - 68 -
3.2.6. Riesgos y amenazas en los SACI ..... - 75 -
3.2.6.1. Ciber-riesgos ..... - 80 -
3.2.6.2. Ciber-amenazas ..... - 90 -
3.2.6.3. Vulnerabilidades en sistemas de control industrial ..... - 94 -
3.2.7. Gestión del riesgo frente a los ciberataques ..... - 100 -
3.2.7.1. Inventariado de activos (TI-TO) ..... - 103 -
3.2.7.2.Problemática asociada a la ciberseguridad ..... - 108 -
3.2.8. Tendencias y predicciones más significativas a nivel técnico y normativo en los SCI ..... - 112 -
3.3. Marco legislativo y normativo ..... - 118 -
3.3.1. Laboratorios de pruebas ..... - 127 -
3.3.1.1. Laboratorios virtuales y remotos ..... - 133 -
3.4. Honeypots ..... - 135 -
3.4.1. Evolución de los Honeypots ..... - 136 -
3.4.2. Clasificación de honeypots ..... - 138 -
3.5. Conclusiones-resumen ..... - 144 -

Capítulo IV

4. Introducción ..... - 146 -
4.1. Análisis descriptivo de SICERCAI ..... - 149 -
4.2. Importancia de la protección y ciber-resiliencia en SACI ..... - 156 -
4.3. Propiedades y métricas de los SCI resilientes ..... - 157 -
4.4. SICERCAI Metodología, materiales y análisis ..... - 163 -
4.5. Nivel de contribución e innovación de SICERCAI ..... - 167 -
4.6. Transferibilidad ..... - 170 -

4.7. Arquitectura de SICERCAI ..... - 171 -
4.7.1. Subsistema SARLAB ..... - 172 -
4.7.2. Servidor de máquinas virtuales ..... - 174 -
4.7.3. Características técnicas del servidor de MV ..... - 183 -
4.8. Célula Automatización Industrial (CAI) ..... - 187 -
4.8.1. PLC SIMATIC S7 1200 -1214C AC/DC/RLY ..... - 188 -
4.8.2. SCALANCE S615 ..... - 197 -
4.8.3. Sinema Remote Connect ..... - 202 -
4.8.4. SCALANCE W778-1 (SIMATIC NET IWLAN Access Point) ..... - 205 -
4.8.5. Instrumentación incorporada ajena al ámbito industrial ..... - 208 -
4.8.6. HMI (Human Machine Interface) ..... - 210 -
4.9. Desarrollo (TIA Portal Ingeniería, tareas implementadas) ..... - 213 -
4.10. CVSS V3.0 Herramienta para la mejora de la ciber-resiliencia mediante SICERCAI ..... - 219 -
4.10.1. Definición de ecuaciones utilizadas en CVSS ..... - 225 -
4.11. Caso de estudio y análisis tomado como premisa ..... - 228 -
4.12. Resultados y conclusiones ..... - 236 -
4.13. Resumen ..... - 240 -

Capítulo V

5. Introducción ..... - 244 -
5.1. Contenido del estudio llevado a cabo en el CCDCoE ..... - 247 -
5.2. Redes eléctricas inteligentes smart grid ..... - 251 -
5.3. Importancia de la ciberseguridad en sistemas de generación y distribución eléctrica ..... - 252 -
5.4. Del enfoque eléctrico al enfoque de datos y control ..... - 254 -
5.5. Riesgos y amenazas existentes en las smart grids ..... - 256 -
5.6. Protocolos GOOSE, MMS y software IEDScout ..... - 257 -
5.6.1. Debilidades del protocolo GOOSE ..... - 266 -

5.7. Caso de estudio y análisis desarrollados en la investigación llevada a cabo en el CCDCoE ..... - 267 -
5.8. Procedimiento, arquitectura e instrumentación del banco de pruebas utilizado en la investigación ..... - 269 -
5.9. Análisis de los datos del IED del fabricante ABB ..... - 273 -
5.9.1. Análisis de los datos del IED del fabricante ARCTEQ ..... - 280 -
5.10. Resultados y conclusiones alcanzadas del estudio llevado a cabo con los IED, ABB y ARCTEQ ..... - 287 -
5.11. Resumen ..... - 288 -

Capítulo VI

6. Preámbulo ..... - 290 -
6.1. Conclusiones ..... - 291 -
6.2. Líneas futuras de investigación ..... - 293 -
6.2.1. SICERCAI ..... - 294 -
6.2.2. SACI involucrados en generación y transporte eléctrico ..... - 295 -

Capítulo VII

7. Introduction ..... - 298 -
7.1 Information Technologies and Operating Technologies ..... - 302 -
7.2 Convergence of Information Technologies and Operating Technologies ..... - 305 -
7.3 Concept of cybersecurity in industrial environments ..... - 310 -
7.4 Importance of cybersecurity in industrial environments ..... - 312 -
7.5 Cybersecurity and cyber-resilience ..... - 315 -
7.6 Critical Infrastructure ..... - 316 -
7.7 Thesis structure ..... - 318 -
7.8 Synopsis ..... - 321 -
7.9 Chapter 1, summary ..... - 322 -
7.10 Chapter 2, summary ..... - 324 -
7.11 Chapter 3, summary ..... - 327 -

7.12 Chapter 4, summary ..... - 328 -
7.13 Chapter 5, summary ..... - 329 -
7.14 Chapter 6, summary ..... - 331 -
7.15 Chapter 7, summary ..... - 332 -
7.16 Final conclusions ..... - 333 -
7.17 Future lines of research ..... - 335 -
7.17.1 SIKRECIA ..... - 335 -
7.17.2 ACSI involved in electric generation and transport ..... - 336 -

Lista de figuras

Figura 1. Representación gráfica del modelo de Purdue ..... - 13 -

Figura 2. Pirámide de segmentación en industria según IEC-62443. ..... - 39 -

Figura 3. Gráfico representativo del modelo del marco de la ciberseguridad..... - 56 -

Figura 4. Gráfico representativo de los estados de implementación en una organización del Cyber Security Framework en su versión 1.1. ..... - 57 -

Figura 5. Estados posibles referente a la alineación entre situación real vs situación objetivo. ..... - 58 -

Figura 6. Procesos involucrados en la definición de un sistema de gestión de ciberseguridad industrial. ..... - 64 -

Figura 7. Fases de un ciberataque, modelo de Lockeed M. ..... - 69 -

Figura 8. Imagen obtenida a través de una búsqueda mediante SHODAN. ..... - 69 -

Figura 9. Relación de protocolos industriales reconocidos por SHODAN (modificada de la fuente original: shodan.io). ..... - 71 -

Figura 10. Resultado de la búsqueda con ZoomEye: tipo y marca de servidor. ..... - 72 -

Figura 11. Resultado de la búsqueda con ZoomEye del app:"Siemens Simatic S7-1200 PLC httpd.” ..... - 73 -

Figura 12. Pantalla de control del PLC hallado en la red. Imagen presentada por el servidor web del PLC a través de Internet. ..... - 75 -

Figura 13. Matriz de riesgos. ..... - 83 -

Figura 14. Representación cronológica de los sistemas operativos de TI, especificando los que conviven en la actualidad en los entornos de las TO. ..... - 89 -

Figura 15. Cronograma de los principales ataques dirigidos a SCAI. ..... - 94 -

Figura 16. Gráfico resumen agrupando vulnerabilidades reportadas durante el periodo de estudio 2010 al 2020, agrupadas por fabricantes. ..... - 97 -

Figura 17. Procesos implicados en la ejecución de inventario de activos (a) y (b). .. - 104 -

Figura 18. Tabla comparativa de las necesidades y peculiaridades de las TI y TO.... - 108 -

Figura 19. Resumen de los procesos implicados en la definida cultura de la cibersegurida ..... - 111 -

Figura 20. Representación gráfica de una posible predicción a nivel técnico y legal en ciberseguridad. (modificada de la fuente original INCIBE-CERT). ..... - 116 -

Figura 21. Imagen resumen de las estrategias establecidas por el Gobierno de España 2011-2019. - 121 -
Figura 22. Representación ilustrativa del concepto de defensa en profundidad. - 128 -
Figura 23. Detalle de una posible arquitectura de una Honey Net. - 137 -
Figura 24. Catalogación de sistemas Honeypots (modificada de la fuente original: INCIBE-CERT). - 138 -
Figura 25. Despliegue básico de un sistema honeypot con el rol de servidor. - 140 -
Figura 26 Despliegue básico de un sistema honeypot con el rol de cliente. - 141 -
Figura 27. Representación gráfica de una honeypot de alta interacción. - 142 -
Figura 28. Representación gráfica de una honeypot de baja interacción. - 142 -
Figura 29. Ciber-incidentes gestionados durante los años 2018-2019, ambos inclusive (fuente: Centro Nacional de Protección de Infraestructuras y Ciberseguridad CNPIC). - 143 -
Figura 30. Ciber-incidentes años 2018-2019, ambos inclusive, distribuidos por sectores estratégicos (fuente: Centro Nacional de Protección de Infraestructuras y Ciberseguridad CNPIC). - 143 -
Figura 31. Ciclo de Gestión estado ante una ciber-crisis - 147 -
Figura 32. Representación gráfica de la conexión tipo de estructura cliente-servidor (OPC). - 153 -
Figura 33. Célula de Automatización Industrial C.A.I.-1. - 154 -
Figura 34. Diagrama de bloques de un controlador proceso proporcional integral y derivativo (PID) realimentado. - 155 -
Figura 35: Representación gráfica de dependencias de ámbito transversal. - 157 -
Figura 36. Gráfica representativa de las capacidades de resiliencia y estados ante una disrupción. - 159 -
Figura 37. Componentes involucrados en la resiliencia. - 162 -
Figura 38. Definición básica del modelado de una Red Petri. - 165 -
Figura 39. Esquema organizativo según la Sociedad Internacional de Automatización (modificada de la fuente original: ISA). - 168 -
Figura 40. Gráfico correspondiente al Sistema de Infraestructura del Conocimiento para la Experimentación Real mediante Células de Automatización Industrial. - SICERCAI-© - 171 -

Figura 41. Representación gráfica de la estructura funcional de SARLAB (CONEXLAB-DIGEXLAB). - 173 -
Figura 42. Descripción de la interacción de CONEXLAB. - 174 -
Figura 43. Servidor de máquina virtuales a disposición de los usuarios. - 175 -
Figura 44. Diferenciación entre modos y sistemas de virtualización. - 176 -
Figura 45. Gráfico representativo, posible modelo de red con diferentes servicios y modos de acceso. - 182 -
Figura 46. Características técnicas del servidor ESXIvirtualizado con VMware. - 183 -
Figura 47. Gráfico representativo de los recursos de hardware utilizados por el servidor ESXI. - 184 -
Figura 48. Gráfico representativo del rendimiento del host donde se encuentra desplegado el servidor ESXI - 184 -
Figura 49. Características principales de la máquina virtual Ubuntu creada en el servidor ESXI. - 185 -
Figura 50. Características principales de la máquina virtual Windows 11 creada en el servidor ESXI. - 185 -
Figura 51. Características principales de la máquina virtual de auditoría Kali Linux 2021 creada en el servidor ESXI. - 186 -
Figura 52. CAI-1 con identificación de cada componente incorporado de TO y TI. - 187 -
Figura 53. PLC S7 1200, instalados en la CAI-1. - 189 -
Figura 54. Pantalla de configuración de el servidor web del PLC S7-1200. - 190 -
Figura 55. Segmento programación (proceso de encendido de la luz roja). - 193 -
Figura 56. Segmento programación (proceso de parada del semáforo). - 193 -
Figura 57. Segmento programación (proceso de encendido de la luz ámbar). - 193 -
Figura 58. Segmento programación (proceso de encendido de la luz verde). - 194 -
Figura 59. Segmento programación (programación de tiempos intervalos a través de la placa disparadora). - 194 -
Figura 60. Segmento programación (programación de tiempos de intervalos del semáforo) - 195 -
Figura 61. Placa identificativa del PLC S7 1200 - 196 -
Figura 62. Placa de interruptores (entradas digitales). - 196 -
Figura 63. Scalance S615, instalado en la CAI-1. - 197 -
Figura 64. Esquema de conexión de red entre el tunelador VPN (SRC) y el Scalance S615. - 198 -

Figura 65. Pantalla de configuración del SCALANCE S615 con conexión a SRC habilitada. ..... - 199 -
Figura 66. Página principal de configuración del SCALANCE S615. ..... - 201 -
Figura 67. Placa identificativa del SCALANCE S615. ..... - 201 -
Figura 68. Esquematización representativa de la conectividad a través de SRC (Conexiones tipo cliente-servidor). ..... - 202 -
Figura 69. Descripción de una arquitectura de red con un SRC desplegado para conexiones a través de VPN a redes operacionales. ..... - 204 -
Figura 70. Pantalla de identificación de SRC tras el establecimiento de conexión... - 205 -
Figura 71. Imagen correspondiente al SCALANCE W778-1 incorporado en CAI-1. .. - 205 -
Figura 72. Página principal de configuración del SCALANCE W778-1 ..... - 206 -
Figura 73. Página principal de configuración del SCALANCE W778-1 ..... - 207 -
Figura 74. Configuración del DHCP en SICERCAI. ..... - 207 -
Figura 75. Placa identificativa del SCALANCE W778-1. ..... - 208 -
Figura 76. Componentes IT en la CAI-1 así como fuente de alimentación de 24v. .. - 209 -
Figura 77. Componentes TI incorporados en la CAI-1. ..... - 209 -
Figura 78. Diferentes HMI del fabricante SIEMENS. ..... - 210 -
Figura 79. Pantallas principales del HMI correspondiente a los diferentes menús creados para el proyecto. ..... - 211 -
Figura 80. Sistemas de control simulados a través de HMI y TIA Portal. ..... - 212 -
Figura 81. Pantallas del HMI, sistema control de tráfico. ..... - 213 -
Figura 82. Software de ingeniería TIA Portal ..... - 213 -
Figura 83. Imagen correspondientes al árbol del proyecto SICERCAI-1 y variables declaradas (TIA Portal). ..... - 216 -
Figura 84. Contenido MAIN [OB1] del proyecto SICERCAI-1 segmentos 3, y 4. ..... - 216 -
Figura 85. Contenido MAIN [OB1] del proyecto SICERCAI-1, SEGMENTOS 1 y 2..... - 216 -
Figura 86. Contenido MAIN [OB1] del proyecto SICERCAI-1 segmentos 5 y 6..... - 217 -
Figura 87. Imagen correspondiente al árbol de proyecto SICERCAI-2 y variables declaradas (TIA Portal). ..... - 218 -
Figura 88. Contenido MAIN [OB1] del proyecto SICERCAI-2, segmentos 3 y 4. ..... - 219 -
Figura 89. Contenido MAIN [OB1] del proyecto SICERCAI-2, segmentos 1 Y 2. ..... - 219 -
Figura 90. Catalogación de las métricas para la evaluación del riesgo (CVSS)..... - 228 -
Figura 91. Representación gráfica pila OSI y pila TCP/IP. ..... - 230 -
Figura 92. Diagrama de puntuación sobre el objetivo de la métrica. ..... - 239 -

Figura 93 Etapas del recorrido de la energía eléctrica desde puntos de generación hasta su consumo final (modificada de la fuente original: www.ree.es). ..... - 246 -
Figura 94. OSI (Open Systems Interconnection,sistema abierto de interconexión) . - 247 -
Figura 95. Diagrama de funcionamiento herramientas de fuzzing (modificada de la fuente original: INCIBE-CERT). ..... - 250 -
Figura 96. Principales componentes de una infraestructura de medición avanzada (AMI) ..... - 251 -
Figura 97. Esquema-composición de una smart grid (modificada de la fuente original: blog.gruponovelec.com). ..... - 255 -
Figura 98. Modelo genérico de red P2P. ..... - 258 -
Figura 99. Escala de valores y tiempos de transmisión de los eventos (GOOSE)..... - 259 -
Figura 100. Formato de la trama de red en el protocolo GOOSE. ..... - 260 -
Figura 101. Captura de tráfico de red con Wireshark ..... - 261 -
Figura 102. Anatomía correspondiente un nombre de objeto en IEC-61850-8-1. ..... - 264 -
Figura 103. Pantalla principal de IEDScout V.5. ..... - 266 -
Figura 104. Esquema de arquitectura desplegada en el CCDCoE.(investigación)..... - 269 -
Figura 105. Iconos y nomenclatura frecuente de IEDScout. ..... - 270 -
Figura 106. Captura de red con wireshark, previa a la conexión contra el IEDScout. - 271 -
Figura 107. Captura de red con wireshark, posteriori a la conexión con el IEDScout - 271 -
Figura 108. Datos de configuración de IED, mostrados por software de ingeniería. . - 272 -
Figura 109. Relación de características evaluadas en BT01_IED y BT15_I. ..... - 272 -
Figura 110. Pantalla principal IEDScout. ..... - 273 -
Figura 111. Representación gráfica de posible acción del tipo "man in the middle" recreada en el caso de investigación llevada a cabo. ..... - 275 -
Figura 112. Conexión establecida contra el BT01_IED. ..... - 276 -
Figura 113. Captura de tráfico de red con wireshark, contraseña en claro. ..... - 277 -
Figura 114. Historial de estado del IED (Reports). ..... - 277 -
Figura 115. Bloque de atributos del IED (Setting groups). ..... - 278 -
Figura 116. Relación de ficheros del IED (Files). ..... - 278 -
Figura 117. Información referente a modelos de datos en BT01_IED (Data model). . - 280 -
Figura 118. Conexión establecida con BT15_I. ..... - 281 -
Figura 119. Relación de características evaluadas en BT01_IED y BT15_I (II). ..... - 281 -
Figura 120. Captura de tráfico a través de wireshark (contraseña en claro BT15_I). . - 282 -
Figura 121. Información a referente al conjunto de datos (Data set). ..... - 283 -

Figura 122. Cambios de estado de los relés, registrados por IEDScout. ..... - 283 -
Figura 123. Cambios en los atributos registrados por IEDScout. ..... - 284 -
Figura 124. Captura de tráfico de red de origen IED, destino nodo maestro. ..... - 284 -
Figura 125. Captura de tráfico de red mediante wireshark (tráfico en claro). ..... - 285 -
Figura 126. Data model Circuito “abierto”. ..... - 286 -
Figura 127. Identificación del Item Id: (**CGI01TMod%stVal)** a través de captura de paquetes de red mediante wireshark. ..... - 286 -
Figure 128. Logical framework of control hierarchy, according Purdue model. ..... - 308 -

Lista de tablas

Tabla 1. Clasificación de los sectores estratégicos/críticos. ..... - 12 -

Tabla 2. Principales fabricantes y protocolos de comunicación asociados (modificada de la fuente original: etxahun.gitbooks.io). ..... - 50 -

Tabla 3. Comparativa vida media entre los dispositivos de TO & TI. ..... - 52 -

Tabla 4. Relación existente entre factores de riesgo y posibles vulnerabilidades asociadas. ..... - 52 -

Tabla 5. Comparativa carencias y necesidades en seguridad entre TI & TO. ..... - 53 -

Tabla 6. Descripción de las fases identificadas ante la aplicabilidad de NIST-CF en estudio realizado a través de SICERCAI. ..... - 59 -

Tabla 7. Relación de dominios y su respectiva descripción según el modelo de madurez de las capacidades en ciberseguridad. ..... - 61 -

Tabla 8. .Clasificación y resumen de las partes intervinientes en los procesos dentro del marco de actuación. ..... - 64 -

Tabla 9. Tabla resúmen del valor del impacto asociado al porcetaje y en concordancia con su probabilidad. ..... - 82 -

Tabla 10. Tabla resumen de las vulnerabilidades que afectan a productos SIEMENS, con direccionamiento directo a ICSA. ..... - 97 -

Tabla 11. Ejemplo ilustrativo clasificación de activos (modificada de la fuente original:INCIBE-CERT) ..... - 107 -

Tabla 12. Resumen del concepto de holismo aplicado a la ciberseguridad. ..... - 111 -

Tabla 13. Tabla resumen de normas y estándares que afectan a las TI y las TO..... - 126 -

Tabla 14. Principales clasificaciones de laboratorios de pruebas. ..... - 128 -

Tabla 15. Relación de las diferentes alternativas de virtualización existentes en el mercado..... - 179 -

Tabla 16. Identificación de componentes de la CAI-1, de la parte TO y TI. ..... - 188 -

Tabla 17. Tipos de métricas en CVSS y vectores asociados. ..... - 223 -

Tabla 18. Asociación entre métricas, valor de la métrica y valor numérico (CVSS). .. - 224 -

Tabla 19. Escala de criticidad. ..... - 225 -

Tabla 20. Definición de la ecuación Base (CVSS). ..... - 226 -

Tabla 21. Definición de la ecuación Temporal (CVSS)..... - 226 -

Tabla 22. Definición de la ecuación de Entorno (CVSS). ..... - 227 -
Tabla 23. Glosario de términos usados en las ecuaciones. ..... - 233 -
Tabla 24. Ecuaciones de entorno (Métrica base). ..... - 235 -
Tabla 25. Ecuaciones de entorno (Fórmula base)..... - 235 -
Tabla 26. Ecuaciones de entorno (Métricas temporales). ..... - 236 -
Table 27. Comparative table of the different classifications made by different countries for strategic sectors. ..... - 308 -

Lista de ecuaciones

Ecuación 1. Formulación matemática del cálculo de la probabilidad en la matriz de riesgos. ..... - 81 -

Ecuación 2. Formulación matemática del cálculo del impacto de la matriz de riesgos.- 81 -

Ecuación 3. Formulación matemática del cálculo del producto de la probabilidad por impacto. ..... - 82 -

Ecuación 4. Ecuación del cálculo del riesgo real en ciberseguridad. ..... - 84 -

Ecuación 5. Ecuación matemática del cálculo del riesgo temporal añadido en ciberseguridad. ..... - 84 -

Ecuación 6. Ecuación matemática del cálculo del riesgo temporal en ciberseguridad. - 84 -

Ecuación 7. Formulación matemática del cálculo del nivel de absorción (Abs). ..... - 160 -

Ecuación 8. Formulación matemática del cálculo del nivel de envejecimiento (F_{env}). - 160 -

Ecuación 9. Formulación matemática del cálculo del nivel de adaptación (Adp) ..... - 160 -

Ecuación 10. Formulación matemática del cálculo del factor de tiempo de recuperación (R_t). ..... - 161 -

Ecuación 11. Ecuación matemática del cálculo valor de la resiliencia del sistema(Res)- 161 -

Ecuación 12. Vector Base CVSS 3.0. ..... - 233 -

Ecuación 13. Ecuación modificada según el sistema CVSS V3.1. ..... - 239 -

Lista de scripts

Script 1. Fragmento correspondiente al script devuelto tras la ejecución de una búsqueda con ZoomEye..... - 74 -

Script 2. Definición algorítmica para la obtención de la puntuación base en CVSS. - 86 -

Script 3. Árbol de decisión para la obtención de puntuación global del NVD CVSS - 87 -

Script 4. IEC 61850-8-1, especificación del protocolo(modificado de la fuente original: IEC). ..... - 263 -

Script 5. Archivo XML de configuración, correspondiente al IED BT15_I..... - 275 -

Índice de abreviaturas

APT	Advanced Persistent Threat (Amenaza persistente avanzada)
APDU	Application Protocol Data Unit (Unidad de datos del protocolo de aplicación).
AWL	Anweisungs-Liste (Lenguaje de programación con listas) (STL, Statement lists)
BT	Blue Team (Equipo azul)
CAI	Célula de Automatización Industrial
CAT	Cyber Attack Taxonomy (Taxonomía de los ciberataques)
CERT	Computer Emergency Response Team (Equipo de respuesta ante emergencias informáticas
IC	Infraestructura Crítica
ICCF	Industrial Cybersecurity Certification Framework (Marco certificación en ciberseguridad industrial)
CAT	Cyber Attack Taxonomy (Taxonomía de los ciberataques)
CISA	Certified Information Systems Auditor (Auditor de sistemas de información certificados)
CISO	Chief Information Security Officer (Director de seguridad de la información)
CLI	Command Line Interface (Interfaz de línea de comandos)
CPU	Central Process Unit (Unidad central de proceso)
CSO	Chief Security Officer (Jefe de seguridad)
CTIO	Convergencia tecnologías de la información y de la operación
CVE	Common Vulnerabilities and Exposures (Vulnerabilidades y exposiciones comunes)
CVSS	Common Vulnerability Scoring System (Sistema común de puntuación de vulnerabilidades)
DA	Data attributes (Atributo de datos)

DHCP	Dynamic host configuration protocol (Protocolo de configuración dinámica de host)
DHS	Department of Homeland Security (Departamento de seguridad nacional)
DMZ	Demilitarized zone (Zona desmilitarizada)
ENCS	Estrategia Nacional de Ciberseguridad
ESN	Estrategia de Seguridad Nacional
FIRST	Forum of Incident Response and Security Teams (Fórum mundial de equipos de seguridad y respuesta a incidentes)
FUP	Funktionsplan (Lenguaje gráfico de programación basado en bloques)
GSE	Generic Substation Event (Evento genérico de la subestación)
GOOSE	Generic Object Oriented Substation Events (Eventos genérico orientados a objetos de la subestación)
GSSE	Generic Substation State Events (Eventos de estado de la subestación)
HMI	Human Machine interface (Interfaz hombre-máquina)
HN	HoneyNet (Tipo especial de honeypots, los cuales se caracterizan por su alta interacción sobre una red entera de sistemas vulnerables)
HP	HoneyPot (Sistemas hardware o software que simulan equipos o sistemas vulnerables)
ICCF	Introduction to the Framework Certification of Cybersecurity Components (Introducción al marco de certificación de componentes de ciberseguridad)
IED	IED Configuration Description (Configuración y descripción del IED)
IIoT	Industrial Internet of Thing (Internet industrial de las cosas)
IoT	Internet of Things (Internet de las cosas)
JCR	Joint Research Center (Centro conjunto de investigación)
KOP	Kontakplan (Programación mediante diagramas de contactos
LPCI	Ley de Protección de Infraestructuras Críticas

LAN	Local area network (Red de área local)
LPIC	Ley de Protección de Infraestructuras Críticas
MMS	Manufacturing Message Specification
MV	Máquinas virtuales
NIST-CF	National Institute of Standards and Technology Cyber-Security Framework (Marco de ciberseguridad del Instituto Nacional de Normas y Tecnologías)
OpenVas	Open Vulnerability Assessment (Evaluación abierta de vulnerabilidades)
OSSIM	Open Source Security Information Management (Gestión de información de seguridad de código abierto)
PLC	Programmable Logic Controller (Controlador lógico programable)
PROFINET	Process Field Network (Red de campos de procesos)
RAM	Random Access Memory (Memoria de acceso aleatorio)
RDP	Remote Desktop Protocol (Protocolo de escritorio remoto)
RPIC	Reglamento de Protección de Infraestructuras Críticas
RT	Red Team (Equipo rojo)
SARLAB	Sistema de Acceso Remoto a LABoratorios
SACI	Sistemas de Automatización y Control Industrial
SCADA	Supervisory Control And Data Acquisition (Supervisión, control y adquisición de datos)
SCI	Sistemas de control industrial
SCL	Substation Configuration Language (Lenguaje de configuración de la subestación)
SNMP	Simple Network Management Protocol (Protocolo simple de gestión de redes)
SICERCAI	Sistema de Infraestructura del Conocimiento para la Experimentación Real mediante Células de Automatización Industrial
SIAMTIC S7	Modelo de autómata programable del fabricante SIEMENS

SG	Smart Grid (Redes inteligentes)
SGGCI	Sistema de Gobierno y Gestión de Ciberseguridad Industrial
SIEM	Security Information and Event Management (Sistemas de gestión de información y eventos de seguridad)
SRC	Sinema Remote Connect (Software propietario SIEMENS tunelador VPN)
SO	Sistema Operativo
SOC	Security Operation Center (Centro de operaciones de seguridad)
TCP/IP	Transmision Control Protocol / Internet Protocol (Protocolo de control de transmisión / Protocolo de internet)
TI	Tecnologías de la Información
TO	Tecnologías de la Operación
TIA Portal	Totally Integrated Automation Portal (Software de ingeniaría propietario de SIEMENS)
URL	Uniform Resource Locator (LRU, localizador de recursos uniforme, por sus siglas en castellano)
VLAN	Virtual Local Area Network (Red virtual de acceso local)
VPN	Virtual Private Network (Red privada virtual)
WAN	Wide Area Network (Red de área amplia)
WBM	Web Based Management (Gestión basada en la web)

Capítulo I

Introducción

1. Prólogo

A lo largo de la historia, el ser humano ha ido construyendo máquinas que facilitasen su trabajo donde se requerían grandes esfuerzos físicos, o una exposición arriesgada de su seguridad e integridad, consiguiendo así un aumento de la productividad y de la eficiencia. La gran mayoría de autores/investigadores coinciden que la primera máquina inventada por el ser humano fue la rueda. Los autores estiman que se inventó en el V milenio a.C. en Mesopotamia durante el período de El Obeid (hacia el 4500 a. C.) [URL- 01, 2021], en la antigua región conocida como Creciente Fértil, inicialmente con la función de rueda de alfarero. Posteriormente se empleó en la construcción de carros, expandiéndose por el Viejo Mundo junto con los carromatos y los animales de tiro. Usualmente se cree que la rueda migró a Europa y Asia occidental en el IV milenio a.C., y a la cultura del valle del Indo hacia el III milenio a.C. Sin embargo, la rueda de carromato más antigua que se conoce fue hallada en Eslovenia.

Barbieri-Baja, aboga por la existencia de vehículos de origen oriental (China) los cuales poseían ruedas, los cuales fueron datados alrededor del 2000 a.C., aunque su referencia más antigua se fija alrededor del 1200 a.C.

Entre las culturas americanas no prosperó, probablemente por la ausencia de grandes animales que pudieran tirar de los carromatos, y porque las civilizaciones más avanzadas ocupaban terrenos escarpados y de difícil acceso. Han sido encontradas ruedas en objetos olmecas identificados como juguetes que datan de alrededor del 1500 a.C. Posteriormente, se emplearon en la construcción de carretones [URL- 02, 2008].

Dichos artefactos fueron aumentando en complejidad mecánica, como son las palancas, poleas, correas o ruedas dentadas, transformando los movimientos de las diferentes partes de la máquina para conseguir la acción deseada.

Estos cambios, que según el paso del tiempo fueron sucediéndose de manera paulatina, definieron un marco en el cual se estaban viendo involucrados procesos de evolución tecnológica, económica, social y política. Las transformaciones que se produjeron fueron tan profundas que no se había visto un cambio similar en el mundo desde la revolución neolítica[1], acaecida unos 10.000 años antes, cuando se pasó de unas sociedades y economías de carácter rural y agrario a otras urbanas e industriales.

Pero, verdaderamente, el hito que marcaría un salto cualitativo en la definición de "industria", y que hoy en día asociamos a este término, fue la aparición y uso de fuentes de energía para la automatización de los procesos (vapor de agua, electricidad, petróleo), así como la tecnificación[2] de la industria en el siglo XXI, dotando de interconectividad e interoperabilidad a los procesos a nivel global.

Siguiendo la evolución lógica del concepto contemporáneo de industria, puede considerarse que comienza a coger fuerza a finales del siglo XVIII, siendo imparable hasta nuestros días. En este sentido se habla de cuatro grandes revoluciones industriales:

- *La primera revolución industrial,* fechada en 1784, se produce con la aparición de equipos de producción de carácter mecánico impulsados por

[1] Se denomina revolución neolítica a la primera transformación radical de la forma de vida de la humanidad, que pasó de nómada a sedentaria, al concretarse una economía productora basada en la agricultura y la ganadería. Esta expresión se debe a Vere Gordon Childe.

[2] Según la Real Academia Española, tecnificar, en su primera acepción queda definida como la *"introducción de procedimientos técnicos modernos en las ramas de producción que no los empleaban"*. En su segunda acepción es definida como *"hacer algo más eficiente desde el punto de vista tecnológico"*.

agua y la energía procedente del vapor de agua. Su introducción en la imprenta transformó el medio en la herramienta de comunicación primaria. Surge la definición de "Industria 1.0."

- *La segunda revolución industrial,* fechada en el siglo XIX y más concretamente en 1870, se produce con la aparición de la electricidad y el petróleo como fuentes energéticas para la producción masiva. Surge el concepto de la cadena de producción y la división del conjunto del trabajo para ser realizado en tareas más elementales. Aparece la definición de "Industria 2.0."
- *La tercera revolución industrial*, revolución científico-técnica o revolución de la inteligencia, fechada en 1970[3], se produce con la utilización de componentes basados en el uso de sistemas electrónicos y del campo de las tecnologías de la información en sus sistemas de producción. Este movimiento se caracteriza, a su vez, por poseer cinco peculiaridades principales:
    a) Utilización de energías renovables como, por ejemplo, la energía hidráulica, solar o la eólica.
    b) Innovaciones en los medios y procesos de almacenamiento de energía, como el uso de baterías recargables o pilas de hidrógeno.
    c) Por el impulso de la red eléctrica inteligente o red de distribución de energía eléctrica "inteligente" (Smart Grid) [Sarker E., 2021].
    d) El desarrollo del transporte basado en el vehículo eléctrico (vehículos todo-eléctricos, híbridos enchufables e híbridos eléctricos no enchufables) así como el progreso tecnológico de las

[3] Desde la aparición en esta década de las tecnologías descritas, el ser humano es capaz de automatizar todo un proceso de producción sin intervención humana (https://www.desouttertools.com/industry-4-0/news/503/industrial-revolution-from-industry-1-0-to-industrt-4-0).

pilas de combustible, utilizando la electricidad renovable como energía de propulsión. Se da paso al comienzo de la era de la "Industria 3.0."

- *La cuarta revolución industrial*, datada en el año 2011, se origina con la irrupción de los sistemas físicos cibernéticos para la producción automatizada e interconectada. Esto implica la promesa de una nueva revolución que combina técnicas avanzadas de producción y operaciones con tecnologías inteligentes que se integrarán en las organizaciones, las personas y los activos. Surge la definición de "Industria 4.0."

Por último, y como aclaración, la automatización se postula como pieza clave para diferenciar la etapa actual, la 4ª revolución, de la 3ª revolución industrial. Con una conectividad máxima y un poder informático-computacional extremo, la automatización será fundamental para el cambio de era industrial.

Viniendo a otorgar mayor claridad a lo expuesto, las máquinas en la Industria 4.0 funcionan de forma autónoma sin la intervención de un ser humano, mientras que en la Industria 3.0 las máquinas sólo se encontraban automatizadas[4].

Esta revolución está marcada por la aparición de nuevas tecnologías como la robótica, la minería de datos, la inteligencia artificial, las tecnologías cognitivas, la nanotecnología y el Internet de las Cosas (Internet of Things, IoT, por sus siglas en inglés) viniendo a agregar mecanismos electrónicos y sensores a los dispositivos, y consiguiendo así aumentar sus capacidades tecnológicas y funcionales [Fernández R., 2020]. El propósito principal que se persigue con este tipo de complementos es la recopilación de datos, su análisis y la materialización de acciones automatizadas a gran escala. Cuando

[4] Según la Real Academia Española, automatizar es *"aplicar la automática a un proceso o a un dispositivo"*.

se aplica a la industria puede denominarse Internet industrial de las cosas (Industrial Internet of Things, IIoT, por sus siglas en inglés).

Actualmente, la 4ª revolución industrial se encuentra en pleno apogeo, al ser el periodo de la intercomunicación y de la conectividad el hito diferenciador en su desarrollo. Cabe resaltar respecto a la conectividad, que ya hay más de 7 mil millones de dispositivos móviles conectados a cientos de millones de personas [URL- 03, 2020]. A su vez también existen más de 22.000 millones de dispositivos (o máquinas) conectados a través de Internet (automóviles, teléfonos, hogares, maquinaria, aviones, camiones, barcos, maquinaria de servicios, etc.). Además, con la llegada e implantación de la tecnología 5G existirán más dispositivos que se podrán conectar a los diferentes sistemas. Se prevé que para el año 2025 el número de dispositivos conectados a Internet supere los 38.000 millones [URL- 04, 2020].

1.1. Tecnologías de la Información y Tecnologías de la Operación

Como ha quedado detallado en la sección anterior, la irrupción y evolución de las diferentes revoluciones industriales ha propiciado que en cada una de ellas hayan aparecido nuevas tecnologías. Así, se puede observar cómo desde la primera revolución industrial en la que se crean máquinas que conjugan elementos mecánicos para el ahorro de esfuerzos (poleas, engranajes, etc.) junto a elementos de propulsión (vapor de agua), la sociedad ha evolucionado hacia la 4ª revolución industrial, donde se potencia el aprovechamiento de las tecnologías de las comunicaciones y de

la computación, utilizando protocolos de comunicación y de redes de última generación, como pueden ser las redes de intercomunicación 5G[5].

Fruto de esta diferenciación por su especialización surgen los conceptos definidos como Tecnologías de la Información (TI[6]) y Tecnologías de la Operación (TO[7]). Se pueden considerar y definir como ideas diferentes pero no excluyentes. Antes de profundizar en la definición de estos dos conceptos, existen varios aspectos básicos que se mencionan a continuación, y que vienen a recalcar las principales características diferenciadoras existentes entre ellas:

- *Tecnologías*

Una de las principales diferencias corresponde a la propia tecnología predominante en cada entorno. Mientras que en el área industrial se especifican y se puede hablar de sensores, controladores, actuadores, cintas transportadoras, mecánica, etc., en la parte de las TI [URL- 05, 2015], se habla de entornos de bases de datos, gestores documentales, directorios de credenciales y permisos, servidores web y de correo, etc. Por estas razones, el conocimiento que poseen los perfiles/usuarios de cada tecnología es completamente diferente y supone un gran distanciamiento entre ellos.

De igual manera, no son comparables las necesidades que demandan cada una de las tecnologías. En el área de las TI se observa que las carencias están asociadas a un entorno de gestión y de delegaciones, donde el número de activos no difiere demasiado con el número de usuarios. Sin embargo, si

[5] El 5G implica una nueva generación de redes de comunicación que vienen a conjugar un aumento de velocidad, menor latencia, mucha mayor flexibilidad en gestión de dispositivos y un considerable menor consumo por parte de esta tecnología.

[6] La Tecnología de la Información (TI) es la aplicación de ordenadores y equipos de telecomunicación para almacenar, recuperar, transmitir y manipular datos, con frecuencia utilizado en el contexto de los negocios u otras empresas.

[7] El área que realiza la gestión de dispositivos, redes y aplicaciones relacionadas con la monitorización y control de procesos industriales es la denominada Tecnología de la Operación (TO).

se habla del entorno de las TO se cuenta con multitud de dispositivos repartidos por un espacio amplio y diseminado,en la mayoría de las ocasiones, y su asociación para administración y gestión, demanda bastantes menos personas en proporción a las TI.

Es importante incidir en que los entornos de producción asociados a las TO tienen de manera inherente, afiliadas condiciones extremas de funcionamiento (temperatura, voltaje, humedad, radiación, etc.), nada comparables a los entornos TI.

- *Perspectiva de seguridad*

Siendo las TO un medio de trabajo donde prima la interacción con máquinas y dispositivos electro-mecánicos, la importancia de la exención del peligro, desde el punto de vista de la seguridad física y del proceso (safety[8]), es primordial. Al hablar de safety se está centrando la definición en la protección del medio ambiente, personas e infraestructuras ante posibles fallos en el proceso. En los sistemas de las TI, al no poner vidas en riesgo, se refiere a una seguridad desde el punto de vista lógico (security[9]), es decir, proteger la información con respecto a cualquier tipo de riesgo que pueda ponerla en peligro, ya sean personas, desastres naturales, deterioro instrumental, etc. Ambos arquetipos de seguridad buscan proteger la confidencialidad, integridad y la disponibilidad de la información de los sistemas en sus entornos [Morante N., 2019]. Pero ambas áreas entienden la seguridad partiendo de enfoques diferentes y, a su vez, persiguen sus objetivos de seguridad de forma desigual. En los entornos de producción, el aspecto crítico a proteger es la disponibilidad, ya que no es permisible una

[8] Término inglés acuñado para la seguridad relacionada con riesgos de origen técnico, laboral o natural.

[9] *Security* es el término inglés acuñado para la seguridad relacionada con riesgos de origen antisocial, es decir, provocados intencionadamente por personas para causar daño a otras personas, a bienes patrimoniales, etcétera.

parada inesperada en la producción (por pérdidas monetarias, posibles catástrofes naturales y humanas, etc.). Mientras que en las TI, la confidencialidad de la información y seguridad en los datos son los aspectos prioritarios.

- *Software-Hardware-Sistemas Operativos*

En los sistemas de control industrial predominan los equipos de propósito especial con sistemas operativos propietarios, a diferencia del mundo de las TI donde predominan sistemas operativos estándar, en su mayoría sistemas basados en arquitecturas Windows[10], así como mucho software comercial instalado en cada ordenador para cubrir las necesidades de los trabajadores (bases de datos, procesadores de texto, software ofimático, etc.). Si se realiza un estudio pormenorizado en el área de las comunicaciones, de igual manera, existen en los entornos de producción protocolos propietarios de los fabricantes de elementos industriales (S7, OPC, Modbus, Profibus, etc.)[11]; mientras que en las tecnologías de la información, por las principales labores que se realizan, se pueden hallar protocolos asociados a la navegación e interconexión web, es decir, HTTP/HTTPS sobre TCP/IP[12].

- *Frecuencia en las actualizaciones*

[10] En 1985, Microsoft publica la primera versión de Windows, una interfaz gráfica de usuario (GUI) para su propio sistema operativo (MS-DOS) que había sido incluido en el PC de IBM y compatibles desde 1981.

[11] Un protocolo de comunicación industrial está compuesto de un conjunto de reglas que permiten las interferencias e intercambios de datos entre varios dispositivos que forman una red.

[12] Grupo de protocolos de red que hacen posible la transferencia de datos en redes, entre equipos informáticos e Internet.

Existe una gran diferencia entre la frecuencia de ejecución de las actualizaciones de los sistemas de las TI y de las TO. El área de las TI, dado su alto perfil de variabilidad tecnológica, ostenta una naturaleza que se torna vulnerable y, por consiguiente, demanda actualizaciones de manera permanente. Al tratarse de entornos más dinámicos es fácil encontrar estos errores y solventarlos. Sin embargo, los sistemas de las TO, por su naturaleza originaria de invariabilidad y aislamiento físico y tecnológico, deben permanecer en marcha durante largos periodos de tiempo, por lo que no pueden ser parcheados de manera frecuente, ya que esto requeriría de un reinicio o situaciones de paradas de los sistemas, no asumibles en entornos de producción. Si estos sistemas se desactivan, entonces se detendrían todos los procesos productivos con las pérdidas económicas y posibles riesgos que eso conllevaría. Esta falta de actualizaciones implica que, con una frecuencia demasiado usual en los entornos de las TO, se encuentren desplegados controladores, actuadores, sensores, etc. obsoletos y altamente vulnerables.

1.2. Convergencia de las Tecnologías de la Información y las Tecnologías de la Operación

Una vez aclaradas las principales diferencias entre las TI y las TO en la sección anterior, es necesario dejar clara la convergencia entre ambas tecnologías, y así resaltar la importancia de unas y otras en el seno de la 4ª revolución industrial. Mientras las tecnologías utilizadas en las TO son muy populares para los operadores e ingenieros que trabajan en el sector, su conocimiento es limitado para el personal de las TI.

Tradicionalmente, los entornos de las TI y TO se han tratado de forma separada y aislada, sin interdependencias entre ellas. La distancia existente ha demostrado que la información intercambiada entre estos entornos no ha sido la adecuada, y los importantes beneficios de la concurrencia, como

la comprensión de los riesgos de seguridad y el aumento del rendimiento, exigen mayor atención a todos los niveles. La operación de multitud de industrias, especialmente aquellas englobadas en los sectores estratégicos/críticos de un país, como, por ejemplo, energía, transporte, aguas, área química, investigación, espacio, comunicaciones, etc., son cada vez más dependientes de las comunicaciones y de las redes informáticas.

A continuación, y a modo de resumen, se muestra la Tabla 1, en la que se pueden comparar las diversas clasificaciones llevadas a cabo por diferentes países, en donde se especifican los sectores estratégicos y su referencia web al organismo gestor [URL- 06, 2016].

País	Sectores Infraestructuras Estratégicas/Críticas	Organismo	Referencia
España	**12 Sectores Estratégicos** • *Administración* • *Espacio* • *Industria nuclear* • *Industria química* • *Instalaciones de investigación* • *Agua* • *Energía* • *Salud* • *Tecnologías de la información y las comunicaciones* • *Transporte* • *Alimentación* • *Sistema financiero y tributario*	**C.N.P.I.C.** Centro Nacional para la Protección de Infraestructuras y Ciberseguridad	http://www.cnpic.es
E.E.U.U.	**16 Sectores Estratégicos** • *Químico* • *Comunicaciones* • *Presas/hidroeléctricas* • *Servicios de emergencia* • *Servicio financiero* • *Instalaciones gubernamentales* • *Tecnologías de la información* • *Sistema de transporte* • *Instalaciones comerciales* • *Sector manufacturero* • *Base industrial de la defensa* • *Energía* • *Agricultura y alimentación* • *Sanidad y salud pública* • *Reactores nucleares, materiales y desperdicios radioactivos* • *Agua y depuradoras*	**C.I.S.A.** Cybersecurity & Infrastructure Security Agency	https://www.cisa.gov/critical-infrastructure-sectors

Reino Unido	**9 Sectores Estratégicos** • *Comunicaciones* • *Servicios de emergencia* • *Energía* • *Servicios financieros* • *Alimentación* • *Gobierno* • *Salud* • *Transporte* • *Agua*	**C.P.N.I.** Centre for the Protection of National Infrastructure	https://www.cpni.gov.uk/
Francia	**12 Sectores Estratégicos** • *Alimentación* • *Gestión del agua* • *Energía* • *Finanzas* • *Transporte* • *Comunicaciones electrónicas, audiovisuales e información* • *Industria* • *Sanidad* • *Espacio e investigación* • *Actividades civiles* • *Actividades militares* • *Actividades legales*	**S.G.D.S.N.** Secrétariat Général de la Défense et de la Sécurité Nationale	http://www.sgdsn.gouv.fr/

Tabla 1: Clasificación de los sectores estratégicos/críticos.

El incremento de las comunicaciones, fruto del aumento exponencial de los elementos inteligentes y la necesidad de integrar los datos del proceso en sistemas y aplicaciones corporativas, ha hecho que las TI aparezcan e irrumpan con fuerza en los entornos industriales. Este aspecto queda visiblemente reflejado según el gráfico del modelo de Purdue, con una división clara del marco lógico de la jerarquía de control como se puede observar en la Figura 1.

Figura 1: Representación gráfica del modelo de Purdue.

Muchas empresas han afrontado esta dependencia creando sus propios equipos de soporte dentro de las unidades de negocio, siendo diferentes y estando separados de su propio departamento de TI. De esta acción surgen dualidades entre *tareas-personal* y *recursos-personal* que pueden derivar en problemáticas fruto del desconocimiento de la disgregación funcional y de coordinación y de la falta de entendimiento entre departamentos, cuyas funciones en origen se tornan similares. Estas diferencias y separaciones generan un incremento del riesgo de la gestión y las acciones de cumplimiento, ocupaciones a las que los ingenieros de las TO no están demasiado habituados, y para las que el personal de las TI dispone de sobrada experiencia. Por estas razones, es primordial que ambas áreas se entiendan y colaboren de manera conjunta. Es evidente que tras esta defensa de la integración entre TI y TO se declaren beneficios y se hereden sus peligros asociados.

Como beneficios destacan:

- *Una considerable mejora en la automatización y la obtención de la información notificada por los sensores.*

- *Un aumento del control en las operaciones distribuidas.*
- *Sistemas más eficientes en sus tiempos de respuesta y en su estructura.*
- *Un aumento de la efectividad, la eficiencia y la eficacia debido a una mejor y mayor información*.
- *Perfeccionamiento ante la toma de decisiones basada en una información más precisa en tiempo y forma.*
- *Un aumento de la satisfacción por parte de los clientes, como resultado de los mantenimientos proactivos y la reducción de los tiempos de indisponibilidad.*
- *Avance de la satisfacción de los participantes al disponer de mejores flujos de información.*
- *Objetivos normativos, claros y bien definidos.*

Por otra parte, aparecen los peligros asociados a las TI que, por ende, se trasladan al área de la operación por esa convergencia explicada anteriormente. Los avances en las TI están proporcionando a los sistemas de control industrial una gran capacidad de interconexión, adaptabilidad y extensión de las áreas de producción. Sin embargo, el uso de las redes de comunicación y, esa intercomunicación existente hace que los sistemas de control industrial se vuelvan altamente vulnerables, aumentando, precisamente, su superficie de exposición a posibles ciberataques[13]. Por consiguiente, es esencial desarrollar metodologías para la identificación y el seguimiento de las vulnerabilidades, la clasificación de los sistemas intervinientes y de los activos existentes en las infraestructuras críticas, cualquiera que sea su nivel de complejidad, escalabilidad y heterogeneidad.

[13] Un ciberataque o ataque informático es cualquier maniobra ofensiva de explotación deliberada que tiene como objetivo de tomar el control, desestabilizar o dañar un sistema informático, pudiendo ser el atacante, un individuo o una organización.

1.3. Concepto de ciberseguridad en entornos industriales

Hace aproximadamente dos décadas, numerosas organizaciones pertenecientes a los sectores comercial e industrial comenzaron una evolución digital interconectando sus TI con sus TO.

Parte de esta interconectividad se realizó usando redes públicas de comunicación, como Internet, para los sistemas TI tradicionales. De igual manera, los sistemas TO fueron obteniendo capacidad de conexión proveniente de diferentes dispositivos ajenos al proceso productivo, acorde a su más pura definición, lo cual daría origen al concepto del IoT: sensores, dispositivos endpoint[14], interfaces hombre-máquina (Human Machine Interface, HMI, por sus siglas en inglés), controladores lógicos programables (Programmable Logic Controller, PLC[15]) y unidades terminales remotas (Remote Terminal Unit, RTU[16]).

Durante los últimos años se ha producido una proliferación de dispositivos y tecnologías de IoT, aumentando considerablemente el número de elementos y funcionalidades. Si bien esta interconectividad, ha ayudado a mejorar la colaboración, la fiabilidad, la eficiencia, la disponibilidad, el mantenimiento y la productividad en sus entornos operativos, la ciberseguridad[17] apenas ha sido tenida en cuenta. Esta falta de planificación

[14] Un *endpoint*, también conocido como terminal o punto final, es cualquier dispositivo informático remoto que se comunica con una red a la que está conectado.

[15] Un controlador lógico programable, más conocido por sus siglas en inglés *PLC* (Programmable Logic Controller) o por autómata programable, es una computadora utilizada en la industria, para automatizar procesos electromecánicos, electro-neumáticos y/o electro-hidráulicos.

[16] Una unidad terminal remota (UTR, más conocida por sus siglas en inglés, RTU) es un dispositivo basado en microprocesadores, el cual permite obtener señales independientes de los procesos y enviar la información a un sitio remoto donde se procese.

[17] La seguridad informática, también conocida como ciberseguridad o seguridad de tecnología de la información, es el área relacionada con la informática y la telemática que se enfoca en la protección de la infraestructura computacional y todo lo vinculado con la misma, y especialmente la información contenida en una computadora que se encuentra circulando a través de las redes de computadoras.

ha derivado en un incremento del riesgo a través de la superficie de ataque, ofreciendo más y mejores oportunidades a los atacantes, creadores de código malicioso y a los grupos de cibercriminales, lo cual se ha confirmado a la vista del número de ciberataques exitosos (Black-Energy, WannaCry y Petya [URL- 07, 2018]) que se han producido en diferentes sectores industriales (energía, transporte, manufactura, salud, etc.) a lo largo de los últimos años.

Hoy en día, es común que los ciberataques se lleven a cabo por equipos multidisciplinares con conocimientos de TI y del funcionamiento de la arquitectura tecnológica del sistema industrial objeto del ataque. De esta forma no solo existiría la capacidad de acceder al sistema de control industrial, sino que también se identificarían las partes más críticas y sensibles del proceso industrial, de manera que al sabotearlo se pudieran producir graves daños que afectarían a la producción de la planta industrial, a la propia instalación e incluso repercutir en la salud de las personas.

Ya ha habido casos (por ejemplo, el ciberataque en Ucrania 2015 [URL-08, 2015]) donde los sistemas de control industrial fueron detenidos y dañados debido a que los atacantes comprometieron el entorno de las TO, accediendo a través de las infraestructuras de las TI.

Consecuentemente y, dado el aumento de ciberataques sufridos en las organizaciones, la ciberseguridad ha pasado a ser un asunto importante en la agenda y prioridades de los miembros de las juntas directivas, repercutiendo directamente en un incremento importante de los presupuestos dedicados a ciberseguridad de las TI y TO. Esto viene a marcar un punto de inflexión en el concepto de la seguridad informática como un

proceso partícipe en todas y cada una de las etapas y áreas involucradas en cualquier organización.

Así pues, a modo de resumen y para completar lo expuesto, la seguridad telemática aplicada a la industria del proceso engloba varias acciones, abordando la prevención, monitorización y mejora de la resistencia de los sistemas industriales y su recuperación ante acciones hostiles o imprevistas, que puedan afectar al correcto funcionamiento de los procesos industriales. Por consiguiente debiendo ser considerada esta ciberseguridad industrial como una fase que debe estar presente en todos y cada uno de los ciclos intervinientes en el control industrial.

1.4. Importancia de la ciberseguridad en entornos industriales

En este contexto, otro problema inmerso en el área de la ciberseguridad industrial se corresponde con la ausencia de estándares y regulaciones específicas para las tecnologías del IoT, lo cual dificulta su correcta planificación y ejecución. Además, es posible que algunos modelos de ciberseguridad habitualmente usados en el entorno de las TO no se hayan integrado adecuadamente en el ciclo de vida de los dispositivos y plataformas del IoT, siendo una de las causas de ello sus incompatibilidades, proporcionadas éstas por la antigüedad de los dispositivos [Group I.D.M., 2019].

De manera reiterada, el enfoque de ciberseguridad prevaleciente en el entorno de las TO es recurrir a prácticas y tecnologías correspondientes al área de las TI. Desafortunadamente, esto no siempre funciona y, en algunas ocasiones, han originado problemas con los equipos y dispositivos de las plantas operacionales. Ambos entornos poseen puntos de vista heterogéneos sobre la ciberseguridad y su aplicabilidad ya que tienen

diferentes necesidades de negocio. En consecuencia, se producen aplicaciones erróneas de tecnologías, metodologías o procedimientos habituales en TI en entornos de las TO, lo cual puede producir auto-denegaciones de servicio y otras complicaciones ocasionadas por la propia organización.

A modo de ejemplo, la gestión y uso de recursos y aplicaciones habituales de las TI para realizar las pruebas de intrusión, o las herramientas de mapeo de red[18] pueden afectar los sistemas de las TO, como muestra, los PLC o los RTU antiguos. De manera equivalente, la aplicación tradicional de un software antivirus, antimalware sobre dispositivos de campo, HMI o sistemas de control tradicional, puede incidir sobre su disponibilidad y rendimiento. Si bien es cierto, tal y como se ha comentado, que se ha producido un incremento importante en el número de ciberataques sufridos en todos los sectores de la industria, muy pocos de estos incidentes se han podido relacionar con el ciberespacio, lo cual evidencia significativamente las limitaciones en las capacidades de análisis forense informático en los sistemas de control industrial. Esta carencia se espera que se complique aún más con la llegada de la IoT, en general, y la IIoT en particular.

La monitorización de red por medio de la correlación de eventos de seguridad de extremo a extremo (desde TI hasta TO) constituye una oportunidad para implantar una estrategia de defensa activa e identificación de amenazas para toda la organización. Se asume que muchos procesos industriales necesitarán convivir con productos (tanto dispositivos como aplicaciones) inseguros durante años. Por tanto, uno de los puntos con mayor prioridad a abordar es la identificación prematura y la subsanación de

[18] Realizar un mapeo de red es llevar a cabo una representación gráfica de todas las computadoras y dispositivos en una red mostrando cómo están conectados entre sí.

las brechas existentes en los requisitos de seguridad entre ambos entornos, de cara a desarrollar controles de compensación y previsión, así como constituir un plan integral de ciberseguridad para toda la organización.

Otro aspecto a mejorar es la potenciación, colaboración y creación de equipos multidisciplinares que ayuden a avanzar en esa falta de contribución adecuada y eficiente entre equipos de trabajo de dichos entornos. Además de fomentar sesiones de concienciación y formación diseñadas específicamente para profesionales que vayan a trabajar en la zona de convergencia de las TI y las TO, se tienen que establecer grupos de trabajo multidisciplinares, de forma que todos los aspectos de un problema de seguridad en el ámbito industrial sean considerados. En paralelo, debe desarrollarse una cultura y lenguaje común en un ambiente de cooperación y comprensión mutua ya que nada separa más a las personas que el lenguaje empleado. Es por ello que la gestión de los aspectos culturales constituye el paso previo imprescindible para crear un entorno industrial verdaderamente seguro.

Indudablemente deben ejecutarse pasos decididos y en la dirección correcta para resolver los aspectos y preocupaciones de ciberseguridad referentes a la adopción de nuevas tecnologías y plataformas ofrecidas por la computación en la nube[19] y el IIoT. La complejidad asociada reside, concretamente, en la gestión de la ciberseguridad de los datos, comunicaciones, servicios, etc. aportados por la gran cantidad de dispositivos *"inteligentes"* que se implementarán en entornos industriales.

[19] La computación en la nube (del inglés *cloud computing*), conocida también como servicios en la nube o simplemente «la nube», es un paradigma que permite ofrecer servicios de computación a través de una red, que usualmente es Internet.

Por ello se espera que la superficie de ataque de IIoT se expanda significativamente.

Por último, siendo conscientes de que no existen subterfugios milagrosos y únicos para solucionar los problemas de ciberseguridad asociados a la convergencia de las TI/TO, al menos como plan inicial se sugiere aplicar el siguiente conjunto de medidas:

- *Los controles de seguridad básicos deben implementarse en todas las capas y entornos de la organización.*
- *La ciberseguridad de ambos entornos (TI/TO) debe ser gestionada por un responsable último y debe estar alineada con las directrices marcadas desde la dirección.*
- *Las tecnologías y las amenazas de ambos entornos deben entenderse claramente. Es posible que las tecnologías de las TI no funcionen necesariamente en el entorno de las TO. Además, las amenazas pueden ser diferentes.*
- *Poseer un plan claro de descubrimiento y gestión de activos. Si no se sabe qué se posee, no se podrán conocer sus debilidades y, por consiguiente, sus capacidades de defensa.*
- *Se deben realizar análisis de riesgo periódicos en ambos entornos para identificar vulnerabilidades y garantizar que se implementan los controles de seguridad adecuados.*
- *Las organizaciones deben considerar normativas de ambos entornos como la NIST 800-53 para T I* [URL- 09, 2017], *NIST 800-82* [URL- 10, 2015], [URL- 31, 2021] *e ISA / IEC 62443-1-2* [URL- 11, 2017], *para los Sistemas de Control Industrial (SCI) y las TO.*
- *Desarrollar políticas y procedimientos específicos de SCI que sean consistentes con la ciberseguridad de las TI, la seguridad física y la continuidad del negocio.*

1.5. Ciberseguridad y ciber-resiliencia

Como consecuencia directa de la evolución en la terminología que va irrumpiendo en las TO y por su creciente toma de importancia en roles asumidos por su avance, en esta sección se analiza de forma concisa el concepto de industria ciber-resiliente[20] o con capacidades tecnológicas de resiliencia, por necesidad funcional y de seguridad operacional. Este concepto sirve para calificar a aquel que ostenta la capacidad de prevenir, detectar, contener y recuperar al sistema afectado ante una acción no deseada, minimizando el tiempo de exposición y el impacto o daño final. Como aclaración, se centra el esfuerzo en la continuidad operacional, evitando actos que causen disfunciones en datos, sistemas e infraestructura tecnológicas así como en las redes industriales [Ciberseguridad, 2020].

Este pensamiento se encuentra íntimamente ligado al del ciber-riesgo, al de la ciberseguridad y al de la continuidad operacional de las tecnologías residentes en las zonas de gestión de los sistemas de control industrial. Esto significa no sólo estar preparado para reaccionar frente a situaciones adversas, sino también ostentar la capacidad de ser preventivo ante posibles disrupciones, las cuales son amenazas a estos sistemas.

En este sentido, el estudio presentado en esta Tesis se centra en la obtención de esta característica, la cual dota de una importancia relevante a los entornos industriales por tener una alta cabida de sensibilidad ante la disponibilidad, destacando la capacidad de anteponerse a los futuribles eventos de seguridad lógica, operacional y cibernética.

[20] La resiliencia tecnológica o la también denominada ciber-resiliencia, se corresponde con la capacidad de soportar y recuperarse ante desastres y perturbaciones de un sistema tecnológico.

1.5.1. Infraestructuras críticas

El concepto de infraestructura crítica (IC) otorga un alto índice de diferenciación a aquellas infraestructuras designadas de tal manera, distinguiéndolas de las no catalogadas en ese sentido.

La designación de IC se emplea por los diferentes Estados para detallar, definir y catalogar instalaciones y sistemas sobre los que recaen servicios esenciales de cada uno de ellos, cuya disrupción no permite soluciones alternativas. Su agrupación se realiza intrínsecamente en divisiones estratégicas. Concretamente en España y según la Ley PIC (Ley de Protección de Infraestructuras Críticas), emitida el 8/2011, con fecha de 28 de abril [URL-12, 2011], las IC se encuentran catalogadas y subdivididas en 12 sectores, que son todos aquellos considerados como esenciales para la seguridad nacional o para el conjunto de la economía del país (energético, tecnologías información, transportes, hídrico, salud, alimentación, finanzas, nuclear, químico, investigación, espacial y administración).

El planteamiento de la protección de estas infraestructuras surge como respuesta de los gobiernos ante la necesidad de proteger el complejo sistema de infraestructuras que dan soporte y posibilitan el normal funcionamiento de los sectores productivos, de gestión y de la vida cotidiana de la sociedad.

Los acontecimientos ocurridos durante las dos últimas décadas, p.e. ataques del 11 de septiembre de 2001 (11-S), los atentados terroristas de Madrid del 11 de marzo de 2004 (11-M), a los recientes actos de ciberespionaje, llevados a cabo por Estados (informe Mandiant[21]) [Snaz A., 2021], [URL- 13, 2013] o por espías corporativos, pasando por las amenazas

[21] El informe Mandiant, ofrece una enorme cantidad de información que desvela un gran trabajo (tanto técnicamente como en la cantidad de recursos destinados), y cuya calidad puede considerarse como sólida a nivel técnico.

de Anonymous[22], Wikileaks[23] y los efectos de malware como Stuxnet, han llevado a la mayoría de los gobiernos a incluir en sus agendas el desarrollo de estrategias nacionales de ciberseguridad así como el despliegue de medidas específicas de protección.

Estas incorporaciones en los planes estratégicos gubernamentales convergen para garantizar la seguridad y estabilidad de sus infraestructuras críticas, repercutiendo directamente en la estabilidad social y estatal de cada uno de ellos.

Con ese objetivo fijado y como premisas en las líneas de actuación para la obtención de un plan de acción de protección estratégico y táctico, los distintos países han abordado dicha problemática bajo diferentes perspectivas, pudiéndose agrupar éstas en:

- *Desarrollo de un marco normativo estricto y claramente definido.*
- *Potenciación de las relaciones entre entidades públicas y privadas.*
- *Establecimiento de un marco normativo básico acompañado de una serie de medidas para incrementar las relaciones público-privadas, como complemento a los puntos previos.*

En cualquier caso, el objetivo a alcanzar para la protección de las infraestructuras críticas corresponde al desarrollo, implantación y mejora de las medidas de seguridad oportunas, tanto en su vertiente física como en la lógica/cibernética, y que deben ser acometidas por los operadores

[22] Surgidos del *imageboard 4chan* y del foro *Hackers*; en un comienzo como un movimiento por diversión. Desde 2008 *Anonymous* se manifiesta en acciones de protesta a favor de la libertad de expresión, del acceso a la información, de la independencia de Internet y en contra de diversas organizaciones.

[23] Es una organización mediática internacional sin ánimo de lucro que publica a través de su sitio web informes anónimos y documentos filtrados con contenido sensible en materia de interés público, preservando el anonimato de sus fuentes.

propietarios o responsables de su gestión de cara a garantizar un nivel de protección adecuado.

En este sentido, el Sistema de Infraestructura del Conocimiento para la Experimentación Real mediante Células de Automatización Industrial (SICERCAI) desarrollado como elemento principal de esta Tesis Doctoral, proporciona nuevas aportaciones para la mejora de la investigación, el desarrollo, la simulación y la evaluación del funcionamiento de este conjunto de elementos, así como la capacidad de predecir el comportamiento de un sistema específico en producción industrial real, suministrando valor operativo, táctico y estratégico para la defensa de las IC.

Los diferentes contextos recreados a través de SICERCAI tienen la capacidad de anticiparse a las nuevas amenazas que afectan a los SCI de las infraestructuras críticas. Al ser un sistema abierto, SICERCAI puede utilizar componentes de diferentes fabricantes industriales para cubrir las arquitecturas existentes en la industria de procesos.

Por todo ello, la obtención de altas capacidades de prevención y resiliencia ante las interdependencias existentes entre las infraestructuras críticas, las TI con las TO, así como todos los elementos asociados a estos sistemas de control industrial, son clave y factor crítico de protección de las infraestructuras, porque pueden permitir que un fallo, que parece estar aislado en un ambiente no crítico, consiga producir una disrupción en el sistema o incluso un desplome en cadena, derivando en una posible caída en cascada, siendo esta situación verdaderamente catastrófica para estos entornos.

1.6. Estructura de la Tesis

A continuación, y con el fin de proporcionar la antesala del estudio aquí presentado, se presenta de manera resumida la estructura de la Tesis Doctoral.

En el *Capítulo* 1, y tras una breve introducción en la evolución de los entornos industriales y la clasificación de estos periodos históricos en función de las revoluciones industriales acaecidas, han quedado definidos los conceptos de Tecnologías de la Información y Tecnologías de la Operación, disertando para cada una de esas áreas las problemáticas emergentes como consecuencia de su convergencia y dependencia. Afloran así los conceptos, desconocidos hasta ese momento de ciberseguridad y ciber-resiliencia en el ámbito industrial. Surge la tipificación de los sistemas de control y automatización industrial bajo el amparo legal de su clasificación como infraestructuras críticas. Se produce un punto de inflexión para la catalogación, puesta en escena y protección de esas infraestructuras y sus respectivos sistemas de control tras los atentados terroristas del *11S* ocurridos en 2001[24].

En el *Capítulo* 2 se presentan los objetivos planteados y que sirven de sustento a la investigación desarrollada en esta Tesis. Estos objetivos se desglosan y clasifican en generales y específicos. Como consecuencia de ello se plantean y detallan las hipótesis de partida, dando lugar a las motivaciones proyectadas para la realización de la investigación. El contenido del resto del capítulo trata sobre la descripción de las relaciones necesarias para una

[24] Los atentados del 11 de septiembre de 2001, también llamados por el numerónimo «11S» y «11-S» (en inglés «9/11» «11/9»), fueron una serie de cuatro atentados terroristas suicidas cometidos la mañana del martes 11 de septiembre de 2001 en los Estados Unidos por la red yihadista Al Qaeda que, mediante el secuestro de aviones comerciales para ser impactados contra diversos objetivos, causaron la muerte de 2.996 personas.

adecuada adaptabilidad y efectividad de la infraestructura planteada para la mejora de la ciberseguridad en entornos operacionales de sistemas de automatización industrial. Se detallará al final del capítulo, la metodología desarrollada para la investigación, que se particularizará en el contenido de los capítulos 4 y 5 como resultado de las investigaciones concretas llevadas a cabo.

El *Capítulo* 3 viene a describir un estudio exhaustivo y detallado del estado del arte relacionado con la investigación de la presente Tesis Doctoral. El estudio formulado comienza con el estado actual de madurez de los SCAI, describiendo el análisis realizado de los principales marcos de referencia internacionales para la ejecución y evaluación de la madurez de los sistemas operacionales. Destacan y se han tomado como base, NIST y C2M2 (National Institute of Standars and Technology / Cybersecurity Capability Maturity Model, por sus respectivas siglas en inglés) como ejemplos y referencias tenidas en cuenta para su despliegue en SICERCAI. Seguidamente se hace un estudio detallado del alcance y de las partes implicadas que imitan el área de la investigación por la que se ha optado. Se pormenorizan todas aquellas nuevas exposiciones, vulnerabilidades, amenazas y riesgos a los que los SCI se están viendo abocados, dado su alto grado de interoperabilidad e interconexión. Por último, se dedica el resto del capítulo a la exposición y análisis las de diferentes herramientas y técnicas existentes en la actualidad, para combatir y prevenir posibles disrupciones como consecuencia de ciberataques o configuraciones deficientes y/o erróneas en las TO.

En el *Capítulo* 4 se describe analíticamente la primera de las dos investigaciones realizadas y que se corresponde con el caso planteado como investigación principal desarrollada en esta Tesis. Se comienza llevando a cabo un análisis descriptivo de todos y cada uno de los subsistemas que

componen SICERCAI. El siguiente nivel corresponde y hace mención a la metodología y materiales implementados para su emplazamiento, profundizando en las funcionalidades específicas de manera individualizada. Tras haber realizado un completo análisis funcional, se detalla la programación concreta ejecutada a través de la herramienta de ingeniería tomada como referencia, la cual, facilita la creación y programación de los entornos en SCAI y que se encuentra desplegada y utilizada en contextos industriales. Para finalizar el capítulo se exponen y analizan los resultados obtenidos a través de SICERCAI y CVSS V 3.0 (Common Vulnerability Scoring System, por sus siglas en inglés), como herramientas para la mejora de la ciber-resiliencia, detallando y exponiendo los términos alcanzados.

En el *Capítulo* 5 se describen y estudian varios aspectos prácticos obtenidos como resultado de la investigación desarrollada en el Centro de Ciber-Excelencia de la OTAN, situado en Tallin (Estonia), y que se corresponde con el segundo caso de investigación ejecutado y descrito en la presente Tesis. Este trabajo ha sido desarrollado en el seno de la búsqueda y estudio de vulnerabilidades en sistemas de generación y distribución eléctrica. Se ha optado por la dedicación de un capítulo íntegro a esta investigación, como consecuencia del alto grado de particularidad que posee el sector eléctrico, y concretamente las fases de generación y distribución. Se detallan los resultados obtenidos del análisis de tráfico de red en arquitecturas existentes en las redes inteligentes a través de los diferentes estándares y protocolos de comunicación usados en estas infraestructuras. Para la materialiación de este apartadao y por el carácter y naturaleza especial que ostenta, se hace necesario un entorno específico de ejecución en cuanto a elementos de ingeniería y software de programación industrial para su despliegue y configuración se refiere. Este motivo influyó directamente y fue primordial para llevar a cabo la elección del laboratorio

existente en el Centro de Ciber-Excelencia de la OTAN, (Cooperative Cyber Defence Centre of Excellence, CCDCoE, por sus siglas en inglés) para la investigación detallada en el capítulo 5.

El *Capítulo* 6 resume las principales conclusiones y aportaciones de esta Tesis en el campo de la ingeniería y, concretamente, en el área de la ciberseguridad de los SCAI en infraestructuras críticas, así como las propuestas de una serie líneas futuras de trabajo e investigación.

La presente memoria finaliza con un completo índice bibliográfico, un compendio de apéndices, listados de códigos fuente de programación, referencias a URL de repositorios documentales y un listado de simposios en los que se ha participado como consecuencia de las investigaciones realizadas.

El *Capítulo* 7 representa un resumen general del trabajo desarrollado, transcrito en lengua inglesa, como requisito indispensable por la ostentación del carácter internacional de la presente Tesis Doctoral.

1.7. Resumen

Para llevar a cabo una correcta recapitulación de lo relatado en este primer capítulo, fruto de las investigaciones que en los sucesivos apartados serán detalladas formalmente, se hace necesario introducir históricamente la evolución acaecida en los SCI. Desde el principio de los tiempos, el ser humano ha ido buscando metodologías apoyadas en la creación de herramientas y maquinaria que le facilitasen y le hicieran la vida más cómoda y llevadera. Esto nos ha llevado a ser capaces de ir adecuando nuestra evolución como especie hasta nuestros días.

En este capítulo se ha comenzado otorgando una línea temporal conforme a los principales hechos relevantes asociados a lo que hoy conocemos bajo la definición de “industria”. Esos hitos han dado lugar a las

denominadas revoluciones industriales, que marcan un antes y un después de la adaptación del ser humano a su forma de materializar su trabajo, de una manera más segura y eficiente.

Como consecuencia de estas revoluciones industriales surge un nuevo concepto, que es el de las Tecnologías de la Operación (TO), que vendrá a definirse como la aplicación de la ingeniería[25] para la obtención de una producción más rápida, simple, eficiente y segura.

Ha sido descrita la influencia que está ejerciendo la interacción de las tecnologías de la información (TI) junto a las de la operación, y de ellas mismas por separado, así como la problemática que, desde el punto de vista de la ciberseguridad, está aflorando en la actualidad y en plena expansión de la 4ª revolución industrial por su convergencia y alta conectividad hacia el mundo exterior.

Como consecuencia de esta interconexión, afloran nuevas exposiciones al mundo exterior y, por consiguiente, aparecen las necesidades de protección frente a estos nuevos riesgos, urge la necesidad de potenciar la ciberseguridad y la ciber-resiliencia de las IC.

Finalmente, como avance de la importancia de estos sistemas, se ha descrito el concepto de infraestructura crítica así como su ámbito de aplicabilidad, poniendo como ejemplo la clasificación por la que se ha optado y que han sido desarrolladas en diferentes países, otorgando de esta manera un punto de vista diferente en función a la clasificación, pero confluyendo a la vez en la identificación como IC.

[25] La Ingeniería es la disciplina y profesión que aplica los conocimientos técnicos y científicos y utiliza las leyes naturales y los recursos físicos, con el fin de diseñar e implementar materiales, estructuras, máquinas, dispositivos, sistemas y procesos para alcanzar un objetivo deseado, pero que cumpla con los criterios especificados.

Para la finalización del contenido de la introducción relatada, y con el objetivo fijado de otorgar fluidez a la comprensión de los apartados venideros, se ha detallado capítulo a capítulo su estructura y contenido.

Capítulo II

Objetivos e hipótesis de partida

2. Objetivos

Tras haber realizado una precisa y a la vez intensa introducción en el capítulo anterior sobre la vertiginosa irrupción de las TI en el área del control industrial, surgen nuevas problemáticas asociadas a estos sistemas. De ahí se derivan los elementos que son el apoyo fundamental para sustentar los objetivos esbozados en este estudio.

Los objetivos planteados en esta Tesis se corresponden con la obtención de mejoras de las capacidades de ciberseguridad en ecosistemas compuestos por TI y TO, así como la obtención del conocimiento suficiente para optimizar las capacidades de resiliencia en estos sistemas de naturaleza crítica. Todo ello se concretará en el desarrollo de un método que ponga a disposición de los usuarios todas aquellas herramientas implicadas en los procesos de la industria (software, hardware, ingeniería e instrumentación real desplegada), para así obtener el conocimiento necesario previo a cualquier actualización de equipos desplegados, ejecución y planificación ante nuevas arquitecturas, adquiriendo la capacidad de anticiparse a posibles eventualidades de riesgo no previsto. En la misma línea, se potenciará la capacidad de prever y mitigar posibles fallos, ataques o caídas en cascada de los entornos CTITO.

2.1. Objetivos generales

El objetivo principal de esta investigación es, aprovechando la madurez de las herramientas de ciberseguridad del área de las TI, obtener metodologías y capacidades para desplegar bancos de pruebas, compuestos por elementos de software y hardware provenientes de las áreas de las TI y

de las TO, para mejorar las capacidades de ciberseguridad y ciber-resiliencia de los entornos industriales. De esta forma, se pretende llevar a cabo, la elaboración de una recreación real de los sistemas de control y automatización desplegados en IC, así como el análisis del tráfico de red generado por los protocolos de comunicación, empleados en las infraestructuras de comunicación desplegadas al uso.

Como consecuencia de lo expuesto anteriormente, y en el marco de certificación de la ciberseguridad de los componentes y de los sistemas de control industrial (The IACS Cybersecurity Certification Framework, ICCF[26]), se pretende proponer la posibilidad de incluir el sistema SICERCAI desarrollado en esta Tesis, como una arquitectura más que colabore en el sistema de certificación ICCF, teniendo un lugar por su propia naturaleza dentro del marco europeo, pudiendo llegar a conseguir la identificación como laboratorio de pruebas y certificaciones, y a la vez cumpliendo con las rutas de evaluación coherentes en la estimación, la valoración, ensayos y la certificación [Gómez T., 2021].

2.2. Objetivos específicos

Para lograr la consecución del objetivo principal a continuación se plantean los siguientes objetivos específicos:

- Evaluar la eficacia de una arquitectura específica de TO y TI implementada para su evaluación, la se corresponde con un entorno de producción real, implicado la red de comunicaciones de red y arquitecturas operacionales.
- Desarrollar diferentes patrones de comportamiento bajo la creación de sistemas de evaluación con capacidad para ser incorporados en sistemas

[26] Tiene por objetivo proporcionar la ayuda suficiente para que la certificación en materia de ciberseguridad dentro de la UE sea fluida y fácil, siempre a un costo controlado y con reconocimiento dentro y fuera de las fronteras europeas. https://ec.europa.eu/jrc/en/publication/iacs-cybersecurity-certification-framework-iccf-lessons-2017-study-state-art.

de información de seguridad y administración de eventos (Security Information and Event Management, SIEM, por sus siglas en inglés).

- Dotar de portabilidad a una célula de automatización industrial para una rápida conectividad fuera del ámbito de los laboratorios remotos y virtuales.
- Implementar una alta capacidad de cohesión con tecnologías de diferentes fabricantes a través de protocolos de comunicación (PROFINET PROFIBUS, S7), siendo una opción como posibles líneas futuras de desarrollo.
- Conceder acceso real y remoto al entorno de programación de la célula de automatización industrial (CAI).
- Proporcionar la capacidad de desplegar cualquier sistema operativo cuya misión sea interactuar con el sistema SICERCAI. Gracias a la disponibilidad de un servidor de máquina virtual se dispondrá de un alto número de opciones, dando completa autonomía al usuario del sistema.
- Proporcionar la capacidad de analizar el comportamiento en tiempo real de las vulnerabilidades de los sistemas operativos, de un sistema de control industrial y, lo más interesante, de ambos al mismo tiempo.
- Llevar a cabo un análisis de forma complementaria, en las arquitecturas de red, sistemas de control desplegados para una comunicación eficiente, estándares y protocolos de comunicación, involucrados directamente en el sector eléctrico (enfocado principalmente en las acciones de generación y transporte), dada su importancia y apoyo base para el resto de sectores estratégicos/críticos.
- Desarrollar mecanismos perfectamente determinados, para facilitar e informar de forma legal y conveniente de la detección de algún tipo de vulnerabilidad de “día 0" que se encuentre durante las ejecuciones y estudios de los sistemas operativos de TI.

2.3. Importancia de la ciberseguridad en las TO y en las infraestructuras críticas

Como se ha descrito en el primer capítulo de la Tesis, el concepto de ciberseguridad operacional ha irrumpido en las dos últimas décadas como consecuencia directa de la evolución de los sistemas industriales.

El concepto de ciberseguridad industrial surge principalmente como consecuencia de la unión de los compendios de seguridad del entorno de las TO y los fundamentos de seguridad del entorno de la red de las TI. La ausencia de claridad en este aspecto ha puesto trabas a los usuarios finales para entender e identificar la seguridad como una cuestión crítica que requiere una inversión sistemática y que esté implícita en todos y cada uno de los procesos.

Los avances en las tecnologías de la información están confiriendo a los sistemas de control industrial (SCI) una gran capacidad de interconexión y adaptabilidad. Sin embargo, el uso de las redes de comunicación hace que los SCI sean altamente vulnerables. En consecuencia, es imprescindible desarrollar metodologías para la identificación y clasificación posterior de los SCI que intervengan en activos de infraestructuras críticas con cualquier nivel de complejidad, escalabilidad y heterogeneidad.

En línea con lo anteriormente descrito, los Estados se enfrentan actualmente a diferentes desafíos que confieren a la seguridad nacional un carácter cada vez más complejo. Estos nuevos riesgos ocasionados, en gran medida, por la globalización, y entre los que se cuentan el terrorismo internacional, la proliferación de armas de destrucción masiva o el crimen organizado, se suman a los ya existentes, de los cuales el terrorismo tradicional venía siendo su mayor exponente.

Dentro de las prioridades de la seguridad nacional española se encuentran las infraestructuras estratégicas. Para su protección se hace

imprescindible, por un lado, catalogar el conjunto de aquéllas que prestan servicios esenciales a nuestra sociedad y, por otro, diseñar un planeamiento que contenga medidas de prevención y protección eficaces contra las posibles amenazas hacia tales infraestructuras, tanto en el plano de la seguridad física como en el de la seguridad de las TI y TO.

Las actuaciones necesarias para optimizar la seguridad de las infraestructuras se enmarcan principalmente en el ámbito de la protección contra agresiones deliberadas y, muy especialmente, contra ataques terroristas. Sin embargo, la seguridad de las infraestructuras estratégicas/críticas exige actuaciones que vayan más allá de la mera protección física contra posibles agresiones o ataques, razón por la cual resulta inevitable implicar a otros órganos de la Administración General del Estado, de las restantes administraciones públicas, y organismos del sector privado (empresas demandantes de servicios y fabricantes). Estas infraestructuras críticas dependen cada vez más de las TI, tanto para su gestión como para su vinculación con otros sistemas, para lo cual se basan, principalmente, en medios de información y de comunicación de carácter público y abierto. Es preciso contar, por tanto, con la cooperación de todos los actores involucrados en la regulación, planificación y operación de las diferentes infraestructuras que proporcionan los servicios esenciales para la sociedad (contenido Ley 8/2011 de 28 de abril, BOE 102 de 29 abril).

Todas estas infraestructuras se encuentran compuestas por instrumentación y sistemas que provienen de las TI y TO, y que, dada su extrema madurez en el ámbito de la implantación e interdependencia, se han vuelto altamente vulnerables.

En consecuencia, y dada la incidencia sobre la seguridad de las personas y sobre el funcionamiento de las estructuras básicas nacionales e internacionales, se hace preciso la construcción de planes y estrategias de

análisis de riesgos dirigidos a la mejora de la ciberseguridad y de la ciber-resiliencia, así como el mantenimiento de la estabilidad funcional de todos estos SCI.

El Sistema e Infraestructura de Conocimiento para la Experimentación Real mediante Células de Automatización Industrial (SICERCAI), viene a proporcionar novedosas capacidades para la investigación, el desarrollo, la simulación y el ensayo del funcionamiento de estos sistemas, así como otorgar la capacidad de prever el comportamiento de un sistema concreto en la producción industrial mediante los escenarios recreados a través de SICERCAI.

2.4. Motivaciones de la investigación

La hipótesis de partida planteada en esta Tesis se sitúa en la convergencia entre la teoría analizada, llevada a cabo durante los trabajos de investigación, reflejados en los capítulos 4 y 5, junto con la observación realizada en el ámbito operacional e industrial existente a nivel global. Como puntos de apoyo para la obtención de lo descrito han sido clave las preguntas que se exponen a continuación, las cuales y de manera prácticamente directa, han proporcionado la hipótesis de partida de esta investigación:

I. *¿Cuál es el nivel de ciberseguridad y ciber-resiliencia de un sistema de control industria actual?.*
II. *¿Se posee un conocimiento real de las desventajas en materia de ciberseguridad que se están poniendo de manifiesto debido a la convergencia entre las TI y las TO?.*
III. *¿Qué peso específico posee la ciberseguridad en los entornos industriales?.*
IV. *¿Se debe aplicar la ciberseguridad en las TO como un proceso más en el diseño de los procesos de automatización?.*

v. *¿Verdaderamente los entornos de prueba, laboratorios virtuales/remotos existentes en la actualidad, brindan la posibilidad de cubrir de una manera segura la posibilidad de interactuar con los procesos industriales reales desplegados en IC para su simulación y análisis?.*

vi. *¿Se tendría capacidad de desarrollar un sistema que fuese capaz de aportar conocimiento mediante la experimentación real, empleando células de automatización industrial de naturaleza híbrida, y que a su vez proporcionase nuevas capacidades para la investigación, el desarrollo, la simulación y la prueba del funcionamiento de estos sistemas, así como la capacidad de predecir el comportamiento de un sistema específico en la producción industrial?.*

vii. *¿Qué avances de los alcanzados en la investigación en diseño que se realiza en universidades, centros de investigación e incluso en entornos de producción, podrían incorporarse de forma sencilla y eficaz en un ambiente que mejore la fase de fortificación y resiliencia de los sistemas en el diseño y la mejora de los entornos existentes en operación y los de nueva instauración, sin que sean excesivamente intrusivos?.*

2.5. Clasificación de la hipótesis de partida

Poseer la capacidad de simular y recrear entornos híbridos de sistemas de control industrial en IC, previamente a su puesta en producción, es esencial para tener capacidad para desarrollar metodologías para la identificación y clasificación objetiva de los SCI que intervengan en activos de infraestructuras críticas con cualquier nivel de complejidad, escalabilidad y heterogeneidad. A esta cualidad se le ha otorgado de significado y de identidad propia quedando identificada como *"capacidad de anticipación"*.

Esta cualidad debe ser desarrollada teniendo en cuenta los factores que se detallan a continuación.

2.5.1. Adaptabilidad según necesidad

Ser consciente de las necesidades y adaptarse al nivel de complejidad exigido por el entorno, es imprescindible para una perfecta planificación de medios a emplear y para una optimización de los recursos tanto técnicos como humanos.

Poseer la capacidad de recrear entornos concretos existentes en IC, bajo el paraguas de la convergencia entre elementos de las TI (sistemas operativos de diferentes versiones, niveles de parcheado de seguridad desplegados, etc.) y de las TO (autómatas con una amplia variedad en versiones de firmware, arquitecturas en red, etc.), permitiendo explorar y obtener un amplio campo de visión de las capacidades de diseño y adaptabilidad. Esta cualidad viene amparada según lo recomendado por los estándares de automatización industrial (IEC 62443[27], ISA 99[28], etc.), debiendo ser un paradigma a alcanzar por todas aquellas organizaciones que tengan involucrados en sus líneas de negocio algún SCI, por muy simples que sean.

Actualmente se encuentran validados por el estándar IEC-62443 cinco niveles diferentes en las redes de comunicación industrial, estando implicadas áreas mayoritariamente de las TI (niveles 2, 3 y 4) y zonas de procesos de las TO (niveles 0 y 1).

[27] El estándar IEC 62443 es un conjunto de normas internacionales sobre seguridad informática para redes y sistemas de comunicación industrial.

[28] El comité de desarrollo de normas ISA99 reúne a expertos en ciberseguridad industrial de todo el mundo para desarrollar normas ISA sobre seguridad de sistemas de control y automatización industrial (https://www.isa.org).

En la Figura 2 se puede apreciar la segmentación existente entre estos niveles y su relación funcional.

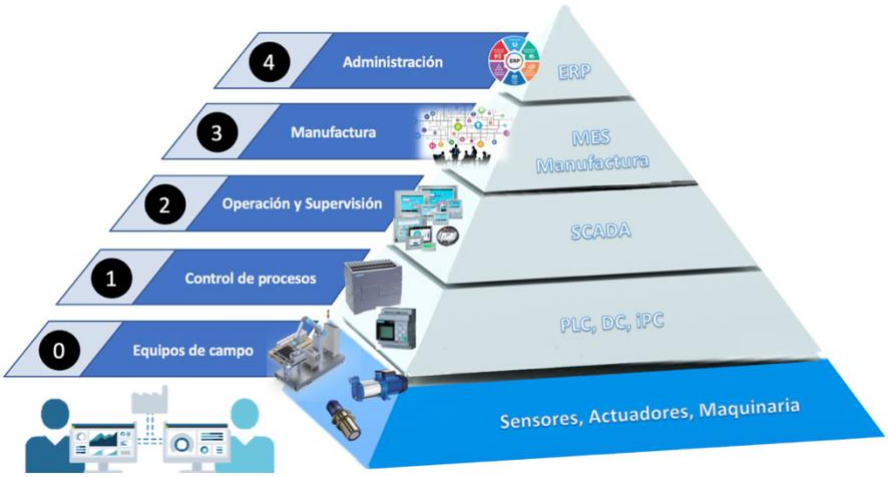


Figura 2: Pirámide de segmentación en industria según IEC-62443.

2.5.2. Efectividad

Otra fase a tener en cuenta a la hora de obtener capacidades de previsión de comportamientos en SCI es el análisis de la efectividad. Este análisis vendría a proporcionar un punto de partida sobre el conocimiento real del estado de la ciberseguridad en el sistema sobre el cual se está trabajando.

La evaluación del tipo de elemento/diseño/sistema puede ser tasada mediante la definición y/o adopción de uno o varios modelos, prácticas y estándares para la comprobación del grado de ciberseguridad y resiliencia del producto diseñado.

Estos modelos, como son el NIST Cybersecurity Framework, C2M2, etc. (descritos en la Sección 3.2), han sido utilizados en esta Tesis como herramienta de evaluación y obtención de un punto de partida de referencia en ciberseguridad para la creación de SICERCAI.

2.5.3. Estructura

El diseño de una estructura a desplegar surge como resultado de un proceso de adaptabilidad y planteamiento correctamente ejecutado. Por consiguiente, un entorno de banco de pruebas orientado a apoyar la etapa de mejora de la ciberseguridad en ingeniería de diseño, debe contener al menos cuatro componentes:

1. *Una célula de automatización industrial,* compuesta por diferentes dispositivos industriales que abarquen el máximo de los procesos a recrear (autómatas, enrutadores, sensores, elementos de interconectividad interna y externa, etc.
2. *Un entorno de ingeniería y programación*, soportado por diferentes sistemas operativos.
3. *Una herramienta de análisis de tráfico de red*, con capacidad de analizar protocolos de comunicación industrial, así como TCP/IP.
4. *Un entorno físico o simulado* (maqueta física o interfaz hombre máquina) en donde se puedan trasladar visualmente las reacciones provenientes de las diferentes pruebas o intrusiones materializadas en el laboratorio.

2.5.4. Método

Apoyándose en la madurez de las herramientas de ciberseguridad procedentes de las TI, y a partir de evaluaciones experimentales de estaciones de ingeniería de los autómatas, software de programación y gestión de los sistemas industriales, experiencia, conocimientos y métodos de trabajo de la ingeniería de procesos, diseño y resultados de la verificación de las arquitecturas evaluadas, así como la creatividad técnica y de la gestión del conocimiento aplicada, es posible identificar elementos y brechas de seguridad relevantes.

Este conocimiento proporciona a su vez información sobre las características particulares de los cuatro componentes mencionados en la hipótesis anterior, tanto de forma individualizada como en el seno de la convergencia entre las TI y las TO.

2.6. Metodología desarrollada en la investigación

En la comunidad mundial, sobre la seguridad cibernética aplicada a SCI, y por consiguiente a las infraestructuras críticas, existe un constante diálogo en el que se producen numerosas propuestas para la mejora de las capacidades en ciberseguridad y ciber-resiliencia de estos entornos.

Prácticamente, en casi todos los ciberataques contra infraestructuras críticas subyacen ciberataques contra sus sistemas de automatización y control industrial. Según informa en su página web el Centro Criptológico Nacional (CCN-CERT) [URL- 14, 2021], los ciber-atacantes están concentrando sus esfuerzos hacia las IC: *"En el punto de mira: las infraestructuras críticas en la era de la ciberguerra"* [CCN-Cert, 2021]. Por lo tanto, es de suma importancia aplicar todas las medidas posibles para aumentar el nivel de ciberseguridad de los sistemas de automatización y control industrial (SACI).

El esfuerzo se debe centrar en la mejora de las capacidades de ciber-resiliencia y ciberseguridad de los componentes individuales y de los sistemas, es decir, desde los dispositivos de campo situados en el "Nivel 0" hasta el estamento jerárquico de más alto nivel de administración "Nivel 4"[29]

[29] Estos niveles de red se encuentran clasificados en "Redes de comunicaciones industriales, Seguridad de la red y del sistema Parte 3-3: Requisitos de seguridad del sistema y niveles de seguridad". Estas divisiones son amparadas por UNE que es el único organismo de normalización en España y como tal actúa como representante de los organismos internacionales ISO/IEC.

pasando por los PLC o los dispositivos de automatización y sistemas de control y adquisición de datos de supervisión (Supervisory Control and Data Acquisition, SCADA, por sus siglas en inglés) [Axel D., 1999], quedando implicados sistemas de hardware, software, comunicaciones e incluso sensores a nivel operacional.

Como aporte para la mejora de la ciberseguridad industrial en todos y cada uno de sus procesos, así como en el conjunto propiciado por la convergencia de las TI con las TO, la investigación desarrollada en esta Tesis se ha centrado en dos áreas fundamentales y que son aplicables a todos los sistemas de control industrial existentes en infraestructuras críticas:

1. *El desarrollo del Sistema de Infraestructura del Conocimiento para la Experimentación Real por medio de Células de Automatización Industrial* SICERCAI. Este sistema proporciona nuevas capacidades para la investigación, el desarrollo, la simulación y la prueba del funcionamiento de cada uno de sus componentes (TI/TO/y arquitectura de despliegue) y, a su vez, del sistema en global y la capacidad de prever el comportamiento de un sistema específico en la producción industrial. Los escenarios recreados a través de SICERCAI tienen la capacidad de anticipar nuevas amenazas que afectan al SCI de las infraestructuras críticas. Usando SICERCAI, una vulnerabilidad conocida de un PLC ha sido verificada a través de la ingeniería programada para el manejo de un sistema de control de semáforos de tráfico. Los resultados obtenidos demuestran la alta dependencia entre los sistemas TI y TO y, por lo tanto, la importancia de poder recrear esos entornos antes de entrar en funcionamiento. Al ser un sistema abierto, SICERCAI puede utilizar componentes de diferentes fabricantes industriales para cubrir las arquitecturas existentes en la industria de procesos.

2. *La búsqueda de vulnerabilidades en SCI en infraestructuras de distribución eléctrica.* Este proyecto fue llevado a cabo en las instalaciones del Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN, que es un centro de ciber-defensa multinacional e interdisciplinario, ubicado en Tallin (Estonia). Cuenta con las instalaciones e instrumentación necesaria para el desarrollo del proyecto *"ICS Vulnerability Research and Pentesting"* (Investigación de Vulnerabilidades y Pentesting[30] en SCI, área de la generación y distribución eléctrica). En esta instalaciones fueron materializados diversos trabajos de investigación cuyo objetivo consistieron en la búsqueda de vulnerabilidades en plataformas y dispositivos de control industrial de los principales fabricantes a nivel mundial desplegados en infraestructuras estratégicas/críticas de generación y distribución eléctrica. Los objetivos planteados en esta parte en concreto fueron varios, dada la envergadura del proyecto, y que a su vez dieron origen al establecimiento de una colaboración en la rama tecnológica implicada en la ciberseguridad de sistemas de control industrial (TI, TO).

2.7. Resumen

En este capítulo se han descrito los trabajos aportados por la investigación desarrollada en la Tesis. Se ha comenzado introduciendo los conceptos de TO y TI a lo largo de la historia de la automatización, describiendo la relevancia de éstas por separado, así como la problemática que, desde el punto de vista de la ciberseguridad, está emergiendo en la

[30] Un *pentesting* es un conjunto de ataques simulados dirigidos a un sistema informático con una única finalidad: detectar posibles debilidades o vulnerabilidades para que sean corregidas y no puedan ser explotadas.

actualidad y en plena expansión de la 4ª revolución industrial por su convergencia y alta conectividad hacia el mundo exterior.

Se ha ido un paso más allá, esclareciendo la relevancia que ostentan estas TO dentro de las infraestructuras críticas nacionales, haciéndolas merecedoras de un profundo estudio sobre sus capacidades de prevención y anticipación frente a un ciberataque, ostentando un papel relevante dentro de los sistemas de certificación propuestos por la Unión Europea.

Como consecuencia de las reflexiones surgidas de esta nueva problemática, han sido detalladas las hipótesis que motivaron la investigación presentada y que dieron lugar a los objetivos de carácter general y específicos que fueron el germen de la estructura seguida en este trabajo de investigación.

Se ha hecho mención a las investigaciones llevadas a cabo y que han conducido hacia la búsqueda de vulnerabilidades en plataformas y dispositivos de control industrial, de los principales fabricantes a nivel mundial y que se encuentran, a su vez, desplegados en infraestructuras estratégicas/críticas de distribución eléctrica. Este sector, el eléctrico es sumamente importante para el resto de sectores estratégicos nacionales e internacionales por su aporte crítico para el funcionamiento del resto de componentes y SACI.

De igual manera, se ha analizado la implicación directa existente entre el pensamiento conservador de ciberseguridad (mediante su aplicabilidad en los entornos de las TI) y el correspondiente al análisis holístico de la definición y aplicabilidad de la ciberseguridad en el ámbito de las TO [Tripathi S., 2021].

A continuación, se han descrito los dos estudios llevados a cabo dentro de la metodología desarrollada y que constituyen el núcleo de esta Tesis. El primero analiza el ámbito de la ciberseguridad industrial de procesos

mediante el análisis de las posibilidades, capacidades de interconexión, adaptabilidad y dependencias creadas por de las TI hacia las TO [González S., 2020]. El segundo estudio aporta los datos obtenidos tras la realización de las pruebas de pentesting y la búsqueda de vulnerabilidades en elementos de control industrial del área de la generación y distribución eléctrica, de diferentes fabricantes y desplegados en la parte de distribución del sector energético de infraestructuras críticas europeas.

Capítulo III

Marco teórico y estado del arte

3. Introducción

Para dar continuidad a la investigación aquí presentada y tras haber consolidado fuertemente los objetivos a alcanzar para la mejora de la ciberseguridad y ciber-resiliencia en los SACI adscritos a IC., en este capítulo se hace necesario ejecutar un estudio de la situación existente en esta materia, para así proporcionar soluciones efectivas y eficientes a las problemáticas subyacentes.

Dada la novedad del área tratada en esta Tesis, en el presente capítulo se detallará la situación concreta y estado actual de todos aquellos actores involucrados en la evaluación, análisis y obtención de propuestas para la mejora de la ciberseguridad de un sistema de control industrial. Este análisis involucra los medios técnicos, los nuevos escenarios acontecidos por la conectividad, los sistemas de evaluación y el análisis de madurez de los sistemas en materia de ciberseguridad, así como la legislación establecida para su regulación y protección a nivel nacional, europeo y transfronterizo.

Como se ha detallado en el capítulo previo, la evolución de la automatización a lo largo de la historia se ha ido encuadrando dentro de las denominadas “revoluciones industriales”. Lo que se puede considerar como la época precedente a la aparición de los primeros controladores lógicos programables estuvo marcada por la incorporación de la electricidad como fuente energética, la cual proporcionaba la potencia necesaria a las máquinas existentes y, lo que fue más importante, propició la incorporación de las bases para los sistemas de control industrial. La aparición de temporizadores, conmutadores contactores y actuadores, accionados por las propias máquinas, interactuaban directamente sobre los motores aplicados

al automatismo, dando lugar a lo que conocemos como tecnologías electromecánicas [Acero G., 1994].

Se fueron añadiendo nuevos componentes a estos sistemas, otorgando la posibilidad de creación de eventos muchos más complejos, pero que, en paralelo, otorgaban sencillez a los procesos facilitados por los entornos mecánicos. Debido a la multitud de los componentes que se incorporaban en paneles de mando y control, se hacía muy complicada su monitorización y sobre todo su mantenimiento. Esto marcó los orígenes del aislamiento originario de los sistemas de control industrial y de la falta de capacidad para su correcto mantenimiento, ya que según iba pasando el tiempo estos sistemas ganaban en complejidad, aislamiento y, por consiguiente, necesidad de durabilidad en el tiempo. Empieza a tomar fuerza la arquitectura de la "seguridad por oscuridad"[31]. Este es un controvertido concepto en el área de la informática, por el cual la ciberseguridad de los sistemas quedaba *garantizada* mediante el ocultismo de una debilidad, en lugar de conocer y proteger el área de exposición al completo [Martínez L., 2009], [Knapp E., 2015].

3.1. Marco metodológico

Según varios autores y, concretamente, para Azuero [Azuero A., 2019], la materialización de un marco metodológico en una investigación se corresponde con ratificar, descubrir y plasmar los casos de estudio, para así poder recrear los datos a partir de los conceptos teóricos que con frecuencia son ejecutados.

[31] Si la seguridad de un sistema depende única o principalmente de mantener oculta una debilidad, entonces, claramente, si esa debilidad es descubierta, la seguridad se compromete fácilmente, no deteniendo el vector de ataque, sino que simplemente es ocultado y sigue estando expuesto a posibles ataques.

Esto viene a significar, para el caso concreto aquí presentado, que se deben especificar cada uno de los aspectos elegidos para el desarrollo en el proyecto de investigación, y que, a su vez, serán justificados a lo largo de la presente Tesis Doctoral. El trabajo aquí mostrado busca la mejora en la ciberseguridad de las TO, así como el respaldo de los miembros de la comunidad de expertos y organizaciones implicadas en materia de ciberseguridad industrial en IC.

3.2. Marco teórico

Como consecuencia directa de esta evolución de los sistemas de las TO, los principales problemas que plantea la ciberseguridad de los entornos industriales son que, en origen, estos fueron diseñados para trabajar de manera ininterrumpida y aislada en cualquier entorno que no correspondiera a aquel para el que fue diseñado, a costa de la eficacia y eficiencia de los sistemas de control industrial, y propiciando este despliegue mediante un diseño robusto, donde su seguridad no estaba asociada al proceso, no permaneciendo en ocasiones ni contemplada.

Es exactamente esa necesidad de durabilidad y disponibilidad lo que ha provocado que hoy en día encontremos en funcionamiento sistemas de control y automatización industrial con una vida superior a quince años, cuya sustitución o actualización, además de provocar pérdidas monetarias por la consecuentes paradas de producción, suele conllevar una fuerte inversión económica por parte de los responsables.

Fabricante	Serie-Modelo	Protocolo
B&R	X20	INA
GENERAL ELECTRIC	Varios modelos	DNP3 /DNP3 SECURE
HITACHI	H SERIES	HI- PROTOCOL
HONEYWELL	UDC 3000	UDC
MITSUBISHI	FX	FX PROTOCOL
OMRON	CJ/CS	FINS
Varios fabricantes	----------	PROFIBUS
Varios fabricantes	----------	PROFINET
ROCKWELL	LOGIC	RS-LOGIC
SCHNEIDER ELECTRIC	TSX	UNITELWAY
SCHNEIDER ELECTRIC	----------	MODBUS
SIEMENS	S7 1200/1500/300/400	S7 MESSAGING
SISTEMAS SCADA (varios fabricantes)	----------	OPC DA
Varios fabricantes	----------	OPC UA

Tabla 2: Principales fabricantes y protocolos de comunicación asociados (modificada de la fuente original: etxahun.gitbooks.io).

Dado que en la mayoría de las ocasiones, la balanza entre producción y seguridad suele inclinarse hacia el lado más lucrativo de la producción, la seguridad queda lastrada de manera evidente. Esto implica que una vulnerabilidad detectada en un elemento concreto pueda estar semanas, meses o incluso años expuesta a un ciberataque, hasta que se realice una parada necesaria y planificada de la producción y se puedan aplicar las correspondientes actualizaciones de seguridad a los elementos vulnerables o incluso proceder a su sustitución [INCIBE-CERT (a), (b), 2015].

Así mismo, a estas exposiciones a la vulneración se incorpora la escasa estandarización de los protocolos de comunicación de los sistemas de control industrial debido a la amplia cantidad de protocolos propietarios. Esto repercute directamente en el incremento de la dificultad de su defensa [Knapp E (a), 2015]. La Tabla 2, viene a resumir y relacionar a los principales

fabricantes de dispositivos de control y automatismos con los protocolos que utilizan para su comunicación.

Por ese motivo se deben efectuar acciones conducentes a la más pura definición del concepto de "ciberseguridad industrial" entendiéndose como tal, al conjunto de prácticas, procesos y tecnologías, diseñadas para gestionar el riesgo del ciberespacio derivado del uso, procesamiento, almacenamiento y transmisión de información utilizada en las organizaciones e infraestructuras industriales, empleando las perspectivas de personas, procesos y tecnologías [Lezzi M., 2018].

3.2.1. Madurez de los sistemas

Como consecuencia de la necesidad de mantener una permanente disponibilidad de los elementos industriales por su naturaleza, y por su coste de montaje y de reposición, tanto de software como de hardware, hacen que su renovación y actualización, en considerables ocasiones, no sean ni siquiera planteados por los responsables de las industrias, y éstos eviten asumir esa acción convencidos de estar sometidos a una baja exposición e invulnerabilidad, [Chen Z., 2020].

Así, por ejemplo, con cierta frecuencia es posible acceder a informes que ponen de manifiesto la existencia de equipos de automatización de los años 90 desplegados en redes industriales actuales [Trend-Micro., 2019]. En contraposición, a día de hoy, no se encuentran sistemas operativos en las áreas de gestión industrial (área corporativa) correspondientes a esas épocas debido a su falta de soporte ante los tipos de software de gestión actuales (paquetes ofimáticos, gestores de bases de datos, software de diseño y maquetación, etc.) [Nexon-Automation, 2019].

Área	Vida Media
Infraestructuras urbanísticas	**30-50** años
Tendido eléctrico	**30** años
Dispositivos de control industrial	**10-20** años
Equipos informáticos (Pc de sobremesa, portátiles, enrutadores, impresoras, pantallas, etc.)	**3-5** años

Tabla 3: Comparativa vida media entre los dispositivos de TO & TI.

Factores de Riesgo	Vulnerabilidades
• **Seguridad por oscuridad**	• Interconexión entre sistemas TI y TO
• **Excesivo ciclo de vida**	• Posibilidad de acceso a infraestructuras desde ubicaciones remotas
• **Segmentación de red**	• SCI, IIOT, SCADA etc. conectados a Internet
• **Configuraciones por defecto**	• Carencia de implicaciones de los profesionales directamente involucrados en diseño, despliegue y mantenimiento
• **Accesibilidad de puertos de conexión**	• Inmadurez/inexistencia de marcos reguladores
• **Aplicaciones-servicios innecesarios**	• Desconocimiento concreto de los activos desplegados en plantas de producción
• **Carencia de políticas de acceso**	• Falta de definición de procesos
• **Falta de gestión de logs**	• Falta de herramientas de seguridad específicas para entornos TO
• **Vulnerabilidades documentadas**	• Uso de la tecnologías de la información de propósito general en sistemas de control industrial
• **Vulnerabilidades “0 Day”**	• Desconocimiento profundo en arquitecturas de redes industriales
• **Inadecuada/carente, política de actualizaciones (software-hardware)**	• Inapropiadas medidas de autenticación (contraseñas por defecto)

Tabla 4: Relación existente entre factores de riesgo y posibles vulnerabilidades asociadas.

Tema de seguridad	Tecnologías de la Información	Tecnologías de la Operación
• **Antivirus**	Ampliamente usado y fácilmente actualizable	Complicado de usar/desplegar y con frecuencia imposible de implementar
• **Ciclo de vida**	3-5 años	10-20 años
• **Sensibilización**	Buena	No buena
• **Administración de actualizaciones**	Frecuente	Escaso, a aprobar por planta en producción
• **Cambio de administración**	Regular y programado	Inusual
• **Análisis de archivos logs**	Práctica establecida y definida	Práctica inusual, no programada
• **Dependencias temporales (funcionalidad)**	Retrasos aceptados en proceso	Inaceptables los retrasos, -Crítico-
• **Disponibilidad**	No siempre disponible, las caídas son ampliamente asumibles	Disponibilidad crítica, 24 x 7 Caídas Inasumibles
• **Test de seguridad**	Ampliamente realizados y programados	Prácticamente nulos problemáticos y peligrosos
• **Test de entorno (despliegue)**	Disponibles, programados con frecuencia	Raramente disponibles

Tabla 5: Comparativa asociada a carencias y necesidades en seguridad entre TI & TO.

Estas diferencias en los períodos existentes de madurez de los elementos industriales ponen de manifiesto la aparición de nuevas vulnerabilidades y factores de riesgo en el ecosistema del control industrial actual. A modo de resumen de lo anteriormente detallado, en la Tabla 3 se relacionan las vulnerabilidades y factores de riesgo a los que se enfrenta la industria a día de hoy, expuesto en términos de tipos de los ciberataques sufridos.

Dada la situación a la que se está viendo abocada la industria y los elementos que la componen, y tras observar la alta disparidad en concepto de necesidades en ciberseguridad entre las TI y TO, (ver Tablas 4 y 5) así como el paradigma emergente resultante de la convergencia de las tecnologías de la información y de la operación (CTIO), se hace necesario un nuevo enfoque

que ayude a establecer unas bases que aporten definición al estado de la ciberseguridad en estos entornos y, por implicación directa, a los sistemas embebidos en infraestructuras críticas. Esto será posible mediante la implantación de un sistema de evaluación de la madurez de los entornos resultantes de la CTIO, cuyo objetivo sea permitir a todas las partes interesadas conocer el grado de madurez y robustez de los controles y medidas de protección implementados en los mismos, procurando especial atención a la importancia que tienen las dependencias en los servicios esenciales y, en particular, a la gestión del riesgo en la cadena de suministro de las TIC.

3.2.2. Principales marcos de referencia de evaluación de madurez de la ciberseguridad en TO

En este subsección se relacionan los principales marcos de referencia de medidas, buenas prácticas, estándares y normativas, que vienen a facilitar la labor del análisis de riesgos en materia de ciberseguridad ubicados en entornos de las TO, y que, a su vez, se encuentran ampliamente utilizados en infraestructuras críticas:

- **C2M2** (Cybersecurity Capability Maturity Model) [Adamu A., 2020].
- **NIST**[32] Cybersecurity Framework 1.1. [Bakare A., 2020].
- **DHS**[33] Catalog of Control Systems Security: Recommendations for Standards Developers [DHS U., 2009].
- **NERC**[34] Critical Infrastructure Protection (CIP) Standards 002-009 [Zafirovic-Vukotic M., 2009].

[32] National Institute of Standards and Technology.

[33] Department Homeland Security USA.

[34] North American Electric Reliability Corporation.

- **NIST** Special Publication 800-82, Guide to Industrial Control Systems Security [Stouffer K., 2015].
- **NIST** Special Publication 800-53, Recommended Security Controls for Federal Information Systems [Initiative J. T. F. T 2014-2020].
- **NIST** Cybersecurity Framework NRC Regulatory Guide 5.71 Cyber Security Programs for Nuclear Facilities [Arinze, U. C, 2016].
- **CNSSI**[35]**,** Committee on National Security Systems Instruction 1253 [Mylrea M., 2017]**.**
- **NISTIR**[36] 7628, Guidelines for Smart Grid Cyber Security [Committee T.S.G.I.P., 2014].
- **ISO**[37] **IEC 27001,** Information Security Management Systems (ISMS) specification.
- **IEC**[38] **62443,** International Standard to establish a cyber security management system (CSMS).

Como apoyo para el diseño y la ejecución del sistema desarrollado en esta Tesis, y del cual se han obtenido las líneas base para el desarrollo de SICERCAI, se analizaron y se aplicaron diferentes etapas y componentes de dos de estos estándares. En concreto el **NIST Cybersecurity Framework 1.1** y el **C2M2 Cybersecurity Capability Maturity Model** [Kaplan A., 2000].

Para facilitar su comprensión y arquitectura operacional se desglosan a continuación las principales características de cada uno de ellos.

[35] https://www.cnss.gov/cnss/

[36] https://www.nist.gov/nist-pub-series/nist-interagencyinternal-report-nistir

[37] https://www.iso.org/standard/54534.html

[38] https://www.iec.ch/homepage

Figura 3: Gráfico representativo del modelo del marco de la ciberseguridad.

3.2.2.1. Marco de ciberseguridad NIST 1.1 (NIST-CF)

El estándar NIST-CF permite obtener la evaluación de la madurez en materia de ciberseguridad de aquellas organizaciones que poseen una convergencia entre las áreas de las TI y TO (infraestructuras críticas, laboratorios industriales de pruebas, etc.) [Stouffer K., 2020], [Dondossola G., 2009]. Este modelo está subdividido en tres áreas fundamentales:

- **Núcleo,** compuesto por el conjunto de categorías y subcategorías que facilitan una comunicación efectiva de los posibles riesgos existentes según queda representado en la Figura 3.

  Define un ciclo completo y continuo en el que quedan completamente identificadas todas y cada una de las etapas ante una gestión de vulnerabilidades. SICERCAI, se encuentra implicado en todas y cada una de las partes mostradas aportando diferenciación significativa frente a lo existente hoy en día.

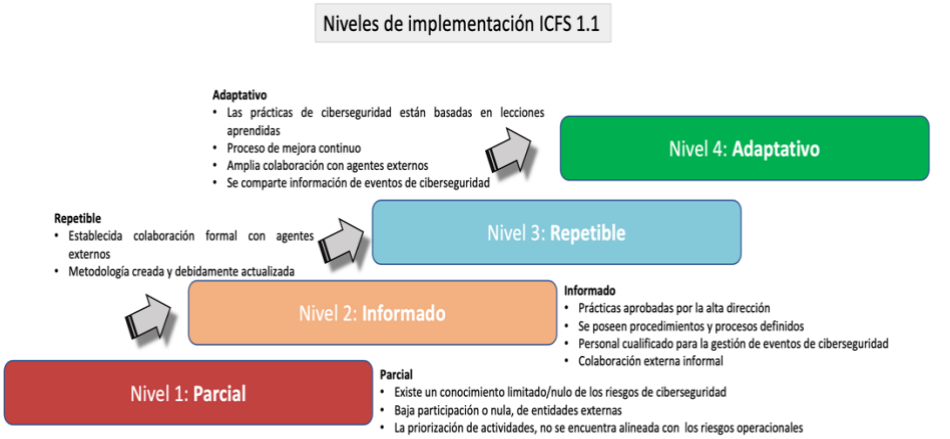
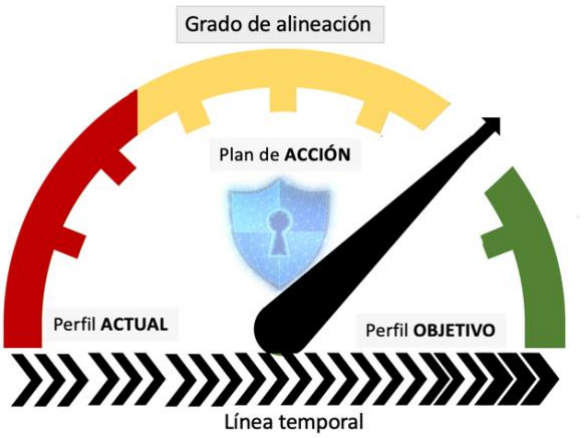


Figura 4: Gráfico representativo de los estados de implementación en una organización del Cyber Security Framework en su versión 1.1.

- **Nivel de implementación**, corresponde al indicador que muestra el posicionamiento de la madurez de la organización con respecto a la ciberseguridad en un momento en concreto, como así se detalla en la Figura 4. Este indicador es aplicable de modo recursivo en todas las etapas descritas en el punto anterior.
- **Grado de alineación,** indica en un momento temporal concreto la relación existente entre el estado de madurez del entorno y un perfil objetivo a obtener, descrito esto en la Figura 5. Esta medida debe ser obtenida y aplicada principalmente en los puntos 2, 3, 4 y 5 (Figura 4), retroalimentado la información existente en la organización, y manteniendo constantemente unos niveles mínimos consensuados en la fase de implementación.

Para el desarrollo de SICERCAI se analizaron diferentes aspectos metódicos proporcionados por NIST-CF. Estos aspectos facilitaron el planteamiento teórico para la creación del sistema, cubriendo así las necesidades planteadas como premisas de esta investigación: la mejora de la ciberseguridad y ciber-resiliencia de los entornos críticos de producción



ayudando a tal objetivo, una alineación equitativa (situación real us objetivo) para obtener un grado de alineación óptimo (ver Figura 5).

Como resultado de este análisis previo realizado, como se puede observar en la Tabla 6 han quedado identificadas un conjunto de fases para una correcta aplicabilidad del marco de la ciberseguridad del NIST. Se han establecido un total de siete fases, las cuales pueden ser modificadas en función al nivel de atomización que se quiera adoptar en el momento de su ejecución.

Figura 5: Estados posibles referente a la alineación entre situación real vs situación objetivo.

Fase	Descripción
Fase 1	Definición del alcance de las mejoras a proporcionar por el sistema SICERCAI (Objetivos)
Fase 2	Identificación de requisitos, carencias existentes, vectores de ataque, principales amenazas. Primera aproximación del estudio del arte
Fase 3	Definición del perfil para evaluación de madurez en entornos concretos (planteamiento para la creación de la primera célula de automatización industrial CAI)
Fase 4	Evaluación de riesgos, aplicabilidad estándar IEC 62443
Fase 5	Definición arquitectura y componentes IT para apoyo al despliegue y obtención de mayor cobertura sobre la casuística planteable
Fase 6	Establecimiento de planes de acción, permisividad de accesos remotos al entorno de pruebas y testeo. Despliegue de máquinas virtuales con diferentes S.O. para entornos de programación de ingeniería y sistemas SCADA

Fase 7	Análisis de una vulnerabilidad concreta de un elemento industrial a través de SICERCAI, capacidad de mejora en ciberseguridad y ciber-resiliencia

Tabla 6: Descripción de las fases identificadas ante la aplicabilidad de NIST-CF en estudio realizado a través de SICERCAI.

3.2.2.2. Modelo de madurez de las capacidades de ciberseguridad C2M2

El modelo C2M2 estableció las bases para complementar la capacidad ya otorgada por NIST-CF al estudio presentado en esta Tesis. Este estándar, propuesto por el Departamento de Seguridad Nacional de los Estados Unidos (Department of Homeland Security, DHS, por sus siglas en inglés), se caracteriza por servir de apoyo y primer paso para la aplicación del NIST-CF.

C2M2 está compuesto por varios dominios de aplicabilidad. La Tabla7, detalla los diez dominios de aplicabilidad y sus correspondientes descripciones, según C2M2 [Kornecki D., 2010]. Estos dominios, muestran y analizan las capacidades de la organización que hace uso del C2M2, cumpliendo así con los criterios especificados en cada uno de ellos. Para la obtención de su valoración se utilizan los indicadores de nivel de madurez o MIL (Maturity Indicators Levels, MIL-0, MIL-1 y MIL-2).

Para la obtención de estos MIL se debe llevar a cabo de manera estructurada la ejecución de las buenas prácticas que se encuentran definidas en el contenido del estándar.

Dominio	Descripción
Gestión del riesgo (GR)	Establecer, operar y mantener un programa de gestión de riesgos de la empresa de seguridad cibernética para identificar, analizar y mitigar los riesgos de seguridad cibernética de la organización, incluyendo sus unidades de procesos productivos, filiales, infraestructura interconectada y las partes interesadas.
Activos, cambio y gestión de la configuración (AGC)	Gestión de las operaciones tecnológicas en la organización y activos de la tecnología de información, que incluye tanto el hardware como el software, el riesgo de la infraestructura y objetivos de la organización.

Gestión de identidad y acceso (GIA)	Crear y gestionar las identidades de acceso lógico o físico a los activos de la organización y las entidades a las que pueden concederse. Controlar el acceso a los activos de la organización, el riesgo de acceso a la infraestructura y objetivos de la organización.
Gestión de las amenazas y las vulnerabilidades (GAV)	Establecer y mantener planes, procedimientos y tecnologías para detectar, identificar, analizar, gestionar y responder a las amenazas de seguridad cibernética y vulnerabilidades asociadas con el riesgo de la infraestructura de la organización (por ejemplo, procesos críticos, activos TI críticos, operativos) y objetivos organizacionales.
Conciencia de la situación (CS)	Establecer y mantener las actividades y tecnologías para recoger, analizar, generar alarmas, presentar y utilizar la información operativa y la seguridad cibernética, incluyendo el estado y la información de resumen de los otros dominios del modelo para formar una imagen operativa común.
Intercambio de información y comunicaciones (IIC)	Establecer y mantener relaciones con entidades internas y externas para recoger y proporcionar información sobre seguridad cibernética, así como las amenazas y las vulnerabilidades para reducir los riesgos y aumentar la capacidad de recuperación operativa, con el riesgo a la infraestructura y objetivos de la organización.
Eventos y respuesta a incidentes, continuidad de las operaciones (RIO)	Establecer y mantener planes, procedimientos y tecnologías para detectar, analizar y responder a eventos de seguridad cibernética y mantener las operaciones a lo largo de un evento de seguridad cibernética proporcionadas al riesgo de la infraestructura y objetivos de la organización.
Cadena de suministro y gestión de dependencias externas (CSGD)	Establecer y mantener controles para gestionar los riesgos asociados a la seguridad cibernética, servicios y activos que son dependientes de entidades externas acorde con el riesgo a la infraestructura y objetivos de la organización.
Gestión del personal (GP)	Establecer y mantener planes, procedimientos, tecnologías y controles para crear una cultura de seguridad cibernética y atención a la adecuación permanente y competencia del personal, con el riesgo a la infraestructura y objetivos de la organización.

Gestión de programas de seguridad cibernética (GPSC)	Establecer y mantener un programa de seguridad cibernética de la empresa que proporciona el gobierno, la planificación estratégica, y el patrocinio de las actividades de seguridad cibernética de la organización, de manera que se alinee con los objetivos de seguridad cibernética, con los objetivos estratégicos de la organización y el riesgo a la infraestructura.

Tabla 7: Relación de dominios y su respectiva descripción según el modelo de madurez de las capacidades en ciberseguridad.

A diferencia del estándar NIST-CF, el C2M2 no requiere de una evaluación de riesgos previa, por lo que incide positivamente en los tiempos de ejecución, siendo estos menos elevados, pero a su vez incide negativamente en la evaluación de la situación en materia de ciberseguridad y ciber-resiliencia. Este es el motivo por el que fue descartado como herramienta principal en esta Tesis.

3.2.3. Alcance de la investigación realizada

Otro punto importante dentro del marco teórico de la presente Tesis se corresponde con la delimitación del alcance de la investigación ejecutada. Para ello se ha acudido a la definición de Sistema de Control Industrial de acuerdo con la International Society of Automation (ISA[39]) que concibe por tal un amplio conjunto de componentes y sistemas que incluyen:

- *Sistemas* SCADA (Supervisory Control and Data Acquisition). Utilizados para un control y adquisición de datos centralizados [Axel D., 1999].
- *Sistemas de Control Distribuidos* (Distributed Control Systems, DCS por sus siglas en inglés). Se trata de una arquitectura compuesta de subsistemas encargada de controlar procesos localizados [Karnouskos S., 2011].
- *Controladores Lógicos Programables*. Dispositivos equipados con memoria no volátil utilizados para controlar equipamientos y procesos [Pérez E., 2009].

[39] International Society of Automation - https://www.isa.org/

- *Sistemas de Seguridad Instrumentados* (Safety Instrumented Systems, SIS por sus siglas en inglés). Controles sobre hardware y software empleados en procesos que impliquen peligrosidad, para advertir o mitigar consecuencias negativas [Asklou N., 2020].

Las particularidades de estos sistemas evidencian la necesidad de un modelo específico centrado en:

- *La seguridad y la disponibilidad.*
- *Las tecnologías específicas y propietarias.*
- *El ciclo de vida del equipamiento*[Office U.S.G.A., 2012].

En el caso de que el nivel de capacidad esté afectado por proveedores de servicios indirectamente relacionados (servicios y coberturas proporcionados por tercero ajenos al proceso base), el responsable del servicio deberá establecer mecanismos para asegurar que dichos terceros cumplen con los requisitos necesarios para el nivel de capacidad definido, así como tener claramente especificados los procedimientos de supervisión, asegurando así que el nivel prevalece durante el tiempo de vida del servicio.

3.2.4. Partes implicadas en los procesos de la ciberseguridad industrial

Dentro de la especificación del marco de actuación es importante la identificación de las partes intervinientes en los procesos. Por definición, como partes implicadas de un sistema en su globalidad, estos roles recaen sobre cualquier individuo, grupo u organización que forme parte o que pueda obtener algún beneficio o perjuicio, y a la vez poseer sus propios intereses operacionales. Como consecuencia directa, queda aclarado que los componentes partícipes en la ciberseguridad industrial revelan diferentes naturalezas.

En la Tabla 8, se especifican de forma resumida las partes intervinientes, diferenciando la clasificación según su modo de implicación (interna, externa o de contribución).

Partes Intervinientes	Necesidad	Función del modelo
Internas		
• **Sistemas de gobierno y gestión**	Conocer el nivel de capacidad para proteger los sistemas de control industrial.	Mejora continua de las capacidades de ciberseguridad de los sistemas de control industrial.
• **Área de operaciones**	Mejorar el nivel de capacidad en los sistemas de control industrial.	Mejora continua de las capacidades de ciberseguridad de los sistemas de control industrial.
• **Responsables de seguridad**	Disponer de un modelo para definir capacidades y roles de ciberseguridad en sistemas de control industrial.	Mejora continua de las capacidades de ciberseguridad de los sistemas de control industrial.
Externas		
• **Consultores auditores**	Disponer de un modelo para definir/evaluar las capacidades de ciberseguridad en el control industrial.	Método para evaluación y mejora continua de las capacidades de ciberseguridad en sistemas de control industrial.
• **Usuarios**	Conocer el nivel de ciberseguridad de los sistemas de control industrial.	Información sobre capacidades ciberseguridad de los sistemas de control industrial.
• **Reguladores**	Conocer el nivel de ciberseguridad de los sistemas de control industrial.	Información sobre capacidades ciberseguridad de Sistemas de Control Industrial.
• **Proveedores**	Disponer de un marco homogéneo para la definición de requisitos.	Evaluación del nivel de capacidad en ciberseguridad de los servicios prestados.
Contribuidora al proceso productivo		

• **Accionistas**	Conocer el nivel de capacidad para proteger los sistemas de control industrial.	Información sobre las capacidades ciberseguridad de los sistemas de control industrial.
• **Socios**	Asegurar niveles equiparables de capacidades en ciberseguridad.	Información sobre las capacidades ciberseguridad de los sistemas de control industrial.

Tabla 8: Clasificación y resumen de las partes intervinientes en los procesos dentro del marco de actuación.

3.2.4.1. Partes intervinientes de carácter interno

- *Sistemas de gobierno y gestión en ciberseguridad industrial (SGGCI)*. Un SGGCI debe estar completamente adaptado y alineado según el tipo de industria en donde vaya a recaer su implantación. Con esta alineación, el beneficio que se obtiene corresponde con una adaptada protección ante las amenazas a las que se puede estar expuesto. Como objetivo, al implantar un SGGCI se propone poner a disposición de la organización todos los recursos disponibles para así lograr una gestión eficiente de los riesgos de ciberseguridad emergentes en los SCI (estos riesgos se detallan en una sección posterior, dada la relevancia e importancia de los mismos).

La Figura 6 viene a esclarecer de manera gráfica los aspectos involucrados en la creación de un SGCI especificando las seis etapas que lo componen.

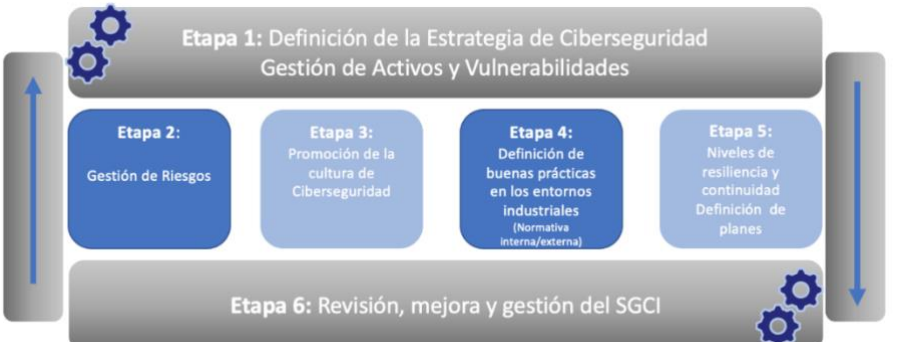


Figura 6: Procesos involucrados en la definición de un sistema de gestión de ciberseguridad industrial.

Etapa 1: Como punto de partida para la creación de un SGGCI, éste debe estar completamente alineado con la estrategia corporativa, definiendo su alcance y la política a llevar a cabo.

Etapa 2: La gestión de los riesgos debe pasar sin lugar a duda por una concreta y concisa metodología de administración de dispositivos (conocimiento de activos, vulnerabilidades y amenazas). Esto quedó reflejado en la Figura 3 de este mismo capítulo, y dada su importancia se le dedicará una sección.

Etapa 3: La promoción de una sólida cultura de ciberseguridad debe fijar sus bases en un desarrollo permanente de formación y concienciación de todos los actores internos, externos y contribuidores implicados en el proceso industrial.

Etapa 4: Creación de la política general de ciberseguridad junto con las normativas aplicables en materia de personas, dispositivos, controles de acceso físico y lógico, control de proceso, seguridad ante riesgos fortuitos e intencionados, así como la protección de la cadena de distribución y de valor en ciberseguridad que comprende la fabricación la distribución y prestación de servicios [URL- 15, 2016].

Etapa 5: El desarrollo y creación de instrumentación y mecanismos para la mejora de la ciber-resiliencia en los SCI, frente a las posibles incidentes que puedan afectar a la continuidad del proceso productivo, actualmente ostenta un papel clave dada la revolución industrial en la que estamos inmersos. SICERCAI incide directamente en esta etapa del SGCI [Zurfluh R., 2021].

Etapa 6: Todo proceso de gestión debe estar sometido a una revisión, supervisión y mejora permanente en el tiempo, evitando así la desinformación y la obsolescencia en la gestión de activos existentes en los entornos productivos [Ganin A., 2020].

- *Área de operaciones*: Uno de los retos que se plantean en los procesos productivos en la Industria 4.0 es la mejora y la optimización de los procesos. Estas mejoras pasan por la reducción de tiempos y costes de producción, eficiencia en los medios a utilizar, adaptación a una producción sostenible y respetuosa con el medio ambiente, y todo ello enfocado a la obtención de un producto mejor. Por ello se debe realizar un análisis pormenorizado de todas y cada una de las actividades y sus respectivas fases, incluyendo la ciberseguridad, entendida en esta área como proceso que afecta a todas las etapas [URL- 16, 2019].
- *Responsables* de seguridad: El papel de coordinador o responsable de ciberseguridad de un entorno industrial debe recaer sobre un trabajador/a de la empresa, siendo su misión principal la gestión y reporte del riesgo a la alta dirección. La figura del responsable de ciberseguridad industrial (Chief Security Officer CSO, por sus siglas en inglés) viene a complementar a la figura del responsable de ciberseguridad corporativa (Chief Information Security Officer CISO, por sus siglas en inglés). Esto es consecuencia directa de la convergencia de los mundos de las TI y TO [URL- 17, 2019].

3.2.4.2. Partes intervinientes externas

- *Consultores auditores:* Las auditorías de ciberseguridad ofrecen a los entornos productivos que buscan proteger sus SCI un mecanismo inicial para evaluar y detectar el estado de madurez en el que se encuentran, verificando y revisando redes, conexiones y flujos de datos.
- *Usuarios*: Los usuarios de los sistemas deben conocer perfectamente no sólo el funcionamiento de los elementos desplegados y operados por ellos, si no, a su vez, los riesgos a los que podrían verse expuestos ante una configuración o manipulación errónea. Deben estar implicados en un

proceso de formación y concienciación permanente. Esta implicación se materializa según la etapa tercera "Promoción de la cultura de Ciberseguridad" del plan de gobierno y gestión.

- *Reguladores*: Como consecuencia directa de la aparición de la 4ª revolución industrial y su fuerte influencia por los medios de interconexión de las TI, se producen nuevos escenarios y necesidades para las cuales no había un marco regulatorio definido. Surgen nuevas iniciativas de ámbito nacionales y europeo dada la importancia de los sistemas de control desplegados en las infraestructuras críticas.
- Proveedores: Disponer de unas medidas adecuadas en ciberseguridad, facilita que los proveedores de materias, instrumentación y de servicios, con los que se interactúa desde la cadena de operación industrial, establezcan una relación de confianza facilitando la fidelización y valor en la producción.

3.2.4.3. Partes intervinientes contribuidoras al proceso productivo

- *Accionistas*: Para aquellas personas que formen parte del conjunto de accionistas de una empresa es de suma importancia que, como consecuencia de todos los procesos detallados con anterioridad, ostenten la seguridad y la confianza de que son copropietarios de una empresa que cumple con unas garantías de ciberseguridad y posicionamiento en el mercado.

- *Socios*: Al igual que un accionista, el socio posee la confianza y seguridad del entorno de producción del cual son parte. La única diferencia existiría desde el punto de vista jurídico[40].

Como referencia y para finalizar esta sección, para llevar a cabo una buena planificación de un SGCI existen varios estándares en los que se han fijado los requerimientos para el desarrollo de SICERCAI. Estos han sido:

- **IEC 62443**, para la definición de procedimientos en los sistemas de CI.
- **ISO 27001**, para la gestión de la seguridad de las TI.
- **ISO 27002**, como guía de buenas prácticas para la mejora de la seguridad de las TI.

3.2.5. Exposición de los sistemas industriales en internet

Como se ha ido relatando a lo largo de las secciones anteriores, la industria se haya en plena interconexión, por lo que se están exponiendo a través de Internet los sistemas de control a una velocidad considerable. Esto, como se ha expuesto en varias ocasiones, comporta una problemática asociada que corresponde al aporte de una información muy valiosa sobre ubicación, fabricante, modelo, versión, etc., del dispositivo en cuestión. Esta información y su obtención, corresponde a la primera etapa en el diseño y ejecución de un posible ciberataque. A modo de resumen la Figura 7 muestra la secuencia a seguir ante un posible ciberataque, ejecutándose éstas de manera secuencial[41].

[40] La diferencia entre socio y accionista radica en que la primera, es una persona que, en parte, es propietaria de un negocio en funcionamiento, y un accionista es una persona que de manera privada tiene una participación de una empresa en forma de acciones compradas a través del mercado de valores.

[41] Modelo obtenido de https://www.incibe.es/protege-tu-empresa/blog/las-7-fases-ciberataque-las-conoces.

Para este reconocimiento y búsqueda de información sobre posibles dispositivos de control industrial expuestos en Internet, dentro de la TI existen multitud de herramientas para la ejecución de esos análisis. Heredadas de las tecnologías de la información surgen varias aplicaciones especializadas para la parte industrial.

Figura 7: Fases de un ciberataque, modelo de Lockeed M.

El proyecto SHINE, conocido como SHODAN (Sentient Hyper-Optimized Data Access Network, por sus siglas en inglés) [URL- 18, 2021], es entre los especialistas en la realización de pruebas de penetración en sistemas muy conocido y utilizado. Es un buscador pensado para encontrar sistemas realizando búsquedas basadas en las respuestas de los banners[42]. Es por eso por lo que es diferente, porque permite buscar texto libremente. Como se

[42] Un banner es una pieza de publicidad digital que combina imágenes, texto y en ocasiones sonido y elementos interactivos, que se introduce en páginas web para dar visibilidad a una marca, empresa o campaña.

puede ver en la Figura 8, tras la realización de una exploración a través de SHODAN y especificando en el campo de búsqueda diferentes palabras clave (SCADA, PLC y RTU), los resultados arrojados son significativos en cuanto a información reportada se refiere (servicios operativos, puertos, protocolos, ubicación física por países, etc.).

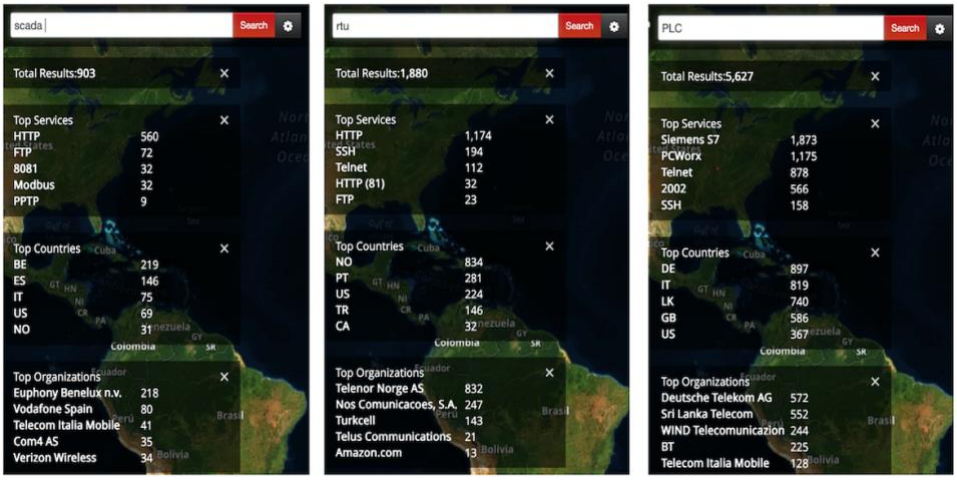


Figura 8: Imagen obtenida a través de una búsqueda mediante SHODAN.

Figura 9: Relación de protocolos industriales reconocidos por SHODAN (modificada de la fuente original: shodan.io).

Este buscador ofrece, a su vez, opciones pre-configuradas de búsquedas complejas para los principales protocolos de comunicación

desplegados en la industria, tal y como se muestra en la Figura 9, lo que facilita enormemente la ejecución de la primera fase ante la preparación de un ataque cibernético enfocado hacia una infraestructura crítica

ZoomEye [URL- 19, 2021] es un motor de búsqueda que se utiliza principalmente para ver dispositivos que son vulnerables. Esta herramienta es accesible a través de un navegador web y permite realizar búsquedas mediante la identificación de protocolos de comunicación industrial, cadenas de texto libre, y por ubicaciones geográficas.

A modo de ejemplo se muestra el resultado de una búsqueda realizada con ZoomEye, siendo el criterio para el hallazgo de un controlador lógico programable el siguiente *"app:"Siemens Simatic S7-1200 PLC httpd".* Los resultados logrados se pueden ver en las Figuras 10 y 11.

A partir de esta búsqueda, y seleccionando cada uno de ellos individualmente, se muestra una relación completa de todos y cada uno de los datos relevantes del dispositivo que ha sido encontrado en la red, con especificación de su dirección IP pública como así se puede observar en la Figura 10. Por motivo de protección de datos, se ha ocultado la dirección IP completa del dispositivo.

Figura 10: Resultado de la búsqueda con ZoomEye: tipo y marca de servidor.

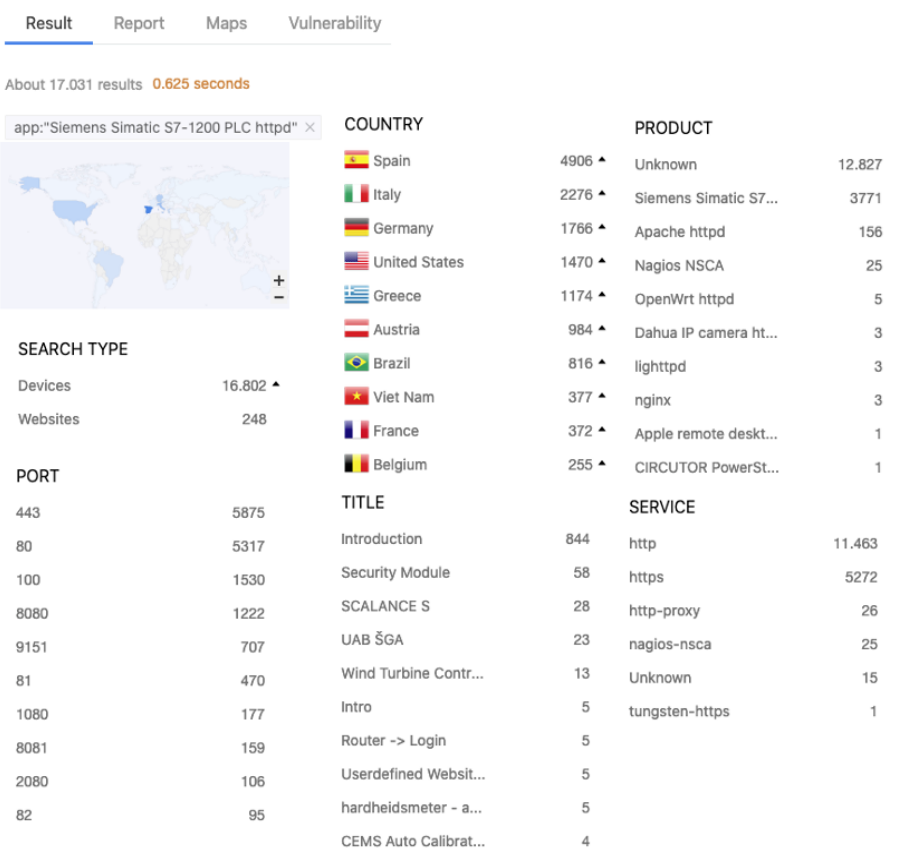


Figura 11: Resultado de la búsqueda con ZoomEye del app:"Siemens Simatic S7-1200 PLC httpd."

En la Figura 11 se muestran los datos adquiridos, siendo de gran importancia los correspondientes al número de dispositivos encontrados (16.802), puertos de conexión abiertos y utilizados para la conexión con especificación de número, producto y servicios habilitados, y la ubicación geográfica.

Un fragmento del script que devuelve la aplicación tras el hallazgo del dispositivo específico encontrado durante la búsqueda en Internet se muestra en el Script 1. El Listado contiene información muy valiosa a la hora de la planificación de un posible ciberataque. El script completo consta de 600 páginas y se encuentra referenciado como anexo y disponible para su posible descarga en el repositorio creado al efecto [URL- 00, 2020].

```
        // Fragmento del contenido del script devuelto por Zoomeye, perteneciente a la ejecución de la búsqueda de uno de los dispositivos hallados
        {
                //var ip ='10.19.XX.XX; //DATO MODIFICADO
                var ip = location.hostname;
                var username = $("username").value; //Identificación usuario
                var password = $("password").value; //Identificación contraseña
                var logintype= $("logintype").value; //Tipo de dato a albergar
                if(gcam==-1)
                        {
                          var r=ocx.LoginDeviceEx(ip,0,username,password,logintype);
                          if (r==1)
                         {
                                        chkdev();
                                        resize();
                                        getcl();
                                        getdjl();
                                        //if (settings['talktype'] != '0')
                                        ocx.SetDeviceMode(0,settings['talktype']);
                                        $('password').value="";
                                        $('l').style.display="none";
                                        $('m').style.top="0px";
                                        settings['username'] = username;
                                        settings['logintype'] = logintype;
                                        savesetting();
                }
                         }
        }
```

Script 1: Fragmento correspondiente al script devuelto tras la ejecución de una búsqueda con ZoomEye.

Tras la obtención de los datos de conexión disponibles y expuestos de forma completamente libre a través de una simple conexión utilizando un navegador, es posible acceder al portal web del autómata descubierto. En este caso en particular se puede verificar la posibilidad de acceder a ciertas funcionalidades del controlador.

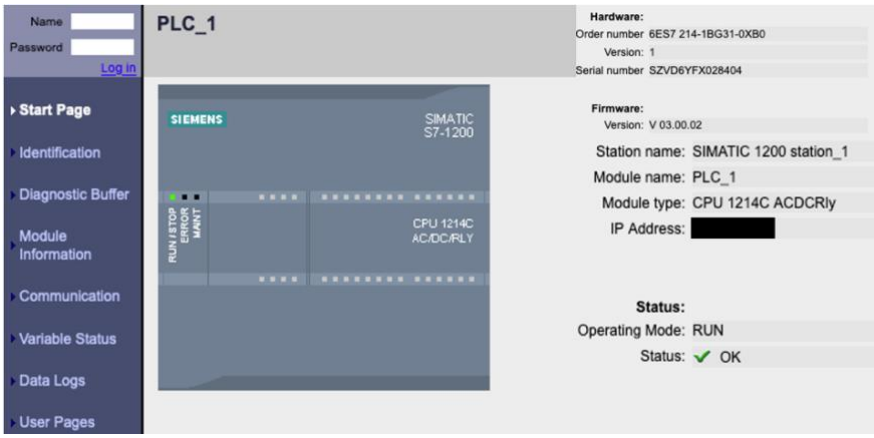


Figura 12: Pantalla de control del PLC hallado en la red. Imagen presentada por el servidor web del PLC a través de Internet.

Como se puede ver a través de la Figura 12, es destacable, como dato de suma importancia, que al poder acceder a este tipo de información, se posee la capacidad de obtener los datos de la versión del firmware[43] instalado en el controlador programable. Precisamente este dispositivo dispone de una versión *no actualizada* de su firmware, concretamente la *V.03.00.02*. Por ello, el PLC se encuentra expuesto a un posible ciberataque manifestando un riesgo considerablemente alto.

En la actualidad, el fabricante, ha liberado la versión 4.4 del firmware [URL- 20, 2021], por lo que se está en la condición de poder afirmar que este dispositivo posee ciertas vulnerabilidades que han sido solventadas por el fabricante y que se encuentran debidamente documentadas y analizadas [URL- 21, 2021].

3.2.6. Riesgos y amenazas en los SACI

El sector industrial está siendo vulnerado por los ataques cibernéticos ocasionados por personas u organizaciones que se aprovechan de los riegos

[43] Es la lógica de más bajo nivel que controla los circuitos electrónicos de un dispositivo de cualquier tipo.

que se encuentran presentes en los elementos de automatización. Estas acciones afectan a los productos, a la calidad en la producción, a la reputación de la marca y a la seguridad de las personas -security-.

Es evidente que existe una necesidad real de integrar en las TO componentes que mejoren las capacidades de protección en lo concerniente a la seguridad en los SCAI.

En [Cherdantseva Y., 2016] y, tras evaluar veinticuatro métodos de estimación de riesgos diferentes, aplicados en el contexto de un sistema SCADA, se pone de manifiesto la necesidad imperiosa de la protección de los mismos ante los ciber-ataques. En [Tascón S., 2020], ante la identificación de estos riesgos y viniendo a mejorar las capacidades de prevención ante los ciberataques en estos sistemas, realiza un estudio en el que propone la implementación del "filtro Kalman" para la mejora de las capacidades preventivas de los SCADA.

Sin embargo, el escenario ha cambiado de forma extraordinaria en la última década y, si bien las medidas existentes siguen cumpliendo su objetivo, existen otras amenazas cuya materialización puede tener efectos tanto o más dramáticos que las ya conocidas y que, sin embargo, no están siendo todavía adecuadamente gestionadas.

Esta carencia de un tratamiento adecuado parece tener su origen en dos aspectos principales relacionados con el conocimiento de las amenazas que afrontan esos sistemas:

1. No se ha generalizado, todavía extensamente, la conciencia de que la apertura e interconexión de los sistemas de control a Internet genera la necesidad de tener en cuenta retos y tecnologías distintas a las que tradicionalmente se venía prestando atención.
2. La percepción de la amenaza no es considerada todavía como cierta y probable en muchos ambientes industriales.

El resultado es la existencia de multitud de sistemas industriales con cuantiosos años de funcionamiento que no han sido diseñados para afrontar los retos de seguridad que plantean las nuevas tecnologías. En ocasiones, estos sistemas han llegado al final de su ciclo de vida, por lo que los fabricantes ya no ofrecen soporte ni actualizaciones de manera periódica.

Cuanto más se prolongue en el tiempo esta dinámica, más aumentará el número de sistemas vulnerables y, en paralelo, más vulnerables serán los sistemas existentes. Por tanto, es necesario actuar y modificar tajantemente este comportamiento para variar esta tendencia.

Para ello, el primer paso es la creación y potenciación de una cultura de ciberseguridad en los entornos industriales, definida en la 3ª etapa del SGCI adoptado en esta Tesis, de forma que los implicados en su diseño, mejora, implantación, adquisición, operación y sustitución sean conscientes de las potenciales problemáticas a las que se están enfrentando y por consiguiente, puedan actuar en consecuencia para tratarlos de forma adecuada y preventiva.

Por ende, y para una efectiva gestión del riesgo, se hace necesario conocer las situaciones que pueden afectar al entorno a fortalecer, es decir, de qué debe protegerse, cuál es su información y sus recursos críticos, y si las medidas que ha implementado para preservarlos evitarán o minimizarán la posibilidad de que se produzca cualquier impacto negativo.

Siguiendo esta línea, en la presente sección se propone el rescatar del olvido ciertos conceptos básicos para conseguir una comprensión de sus implicaciones y así plantear las relaciones que existen entre ellos, alcanzando de esta manera una gestión segura de la CTIO.

- **Vulnerabilidad.** Una vulnerabilidad es una debilidad de un bien o de un control, que puede ser aprovechada por una amenaza. Se trata de una característica negativa del activo o recurso, o de un control que se

implementó sobre él que lo hace vulnerable. En efecto esa vulnerabilidad es susceptible de ser aprovechada y varía de acuerdo con los cambios en las condiciones que dieron origen a su existencia o a las acciones que se tomen con el fin de evitar su explotación o aprovechamiento.

- **Amenaza.** El término amenaza, en contraposición al de vulnerabilidad, requiere reflexionar sobre los problemas a los que el sistema-organización se pueda ver afectado en un futuro cercano, por lo que plantea un posicionamiento anterior a un hecho en concreto, representando a su vez algún grado de probabilidad de materializarse.
- **Riesgo.** La materialización de una amenaza concreta, y que aprovecha una vulnerabilidad, expone a las organizaciones, entornos operacionales y a sus sistemas informáticos a lo que se conoce como riesgo. El riesgo puede ser definido como la posibilidad de que algo que ocurra impacte negativamente sobre la información o sobre los recursos para gestionarla. La norma ISO/IEC-27002, [URL- 22, 2021] lo define como la combinación de la probabilidad de ocurrencia de un determinado hecho y sus consecuencias. Seguidamente por esta materialización descrita surge el impacto, es decir, los hechos o acontecimientos que resultan de uno o varios eventos categorizados. Es importante obtener capacidades de evaluación y clasificación de los riesgos.

El análisis de estos riesgos puede ser realizado de forma cualitativa o cuantitativa. El análisis de riesgos cualitativo se antepone en ocasiones al cuantitativo, a la hora de realizar un estudio exhaustivo de algún riesgo concreto. En otras ocasiones precede directamente a la planificación de respuesta al riesgo, obviándose el análisis cuantitativo. El análisis de riesgos tiene como objetivo establecer una priorización de los riesgos de la organización para ser gestionados posteriormente.

- ***Análisis cualitativo de riesgos***. Este proceso tasa el impacto y la probabilidad de ocurrencia de los riesgos identificados en el proceso, utilizando metodologías y herramientas de análisis de carácter cualitativo. El riesgo se evalúa a partir de dos parámetros: probabilidad e impacto. La probabilidad es la posibilidad de que el riesgo pueda suceder. El impacto o severidad es el efecto sobre los objetivos, en caso de materializarse el riesgo. Todo riesgo viene definido por sus valores de probabilidad e impacto. Si el riesgo puede llegar a materializarse en más de una ocasión, aparece un tercer parámetro de medida, la frecuencia, que tasa el número de veces que un determinado riesgo puede materializarse a lo largo del proceso. Los riesgos deben ser adecuadamente entendidos antes de proceder a la determinación de su probabilidad e impacto. Ello implica someter a examen:
    1. *El grado de conocimiento del riesgo.*
    2. *La información disponible.*
    3. *La calidad e integridad de la información.*
- ***Análisis cuantitativo de riesgos.*** En esta variedad de proceso se utilizan técnicas cuantitativas para determinar la probabilidad y el impacto de los riesgos. Por regla general se ejecuta después del análisis cualitativo de riesgos. Entre las herramientas utilizadas para el análisis cuantitativo del riesgo se encuentran:
    1. **Entrevistas.** La información recogida de los expertos es tratada estadísticamente a partir de los datos de algún parámetro concreto cuyo riesgo se quiera estimar. Los datos solicitados dependerán del tipo de distribución a emplear. Por ejemplo, si se usa una distribución triangular se solicitarán 3 valores correspondientes a los escenarios pesimista, optimista, y más probable.

2. **Análisis de árbol de decisiones.** Se trata de un diagrama que describe una decisión considerando todas las alternativas posibles. Cada rama incorpora probabilidades de riesgos y los costes o beneficios de las decisiones futuras. La resolución del árbol permite reglamentar cual es la decisión que produce el mayor valor esperado. El valor esperado o esperanza matemática se define como el sumatorio de probabilidad por costos y beneficios.
3. **Otros.** Análisis de sensibilidad, simulación utilizando el método del "análisis de Montecarlo". El análisis de Montecarlo es un método utilizado para, mediante una simulación matemática compleja, aproximar el resultado de cálculos de los que no se puede obtener una solución exacta. Es un método que se utiliza para realizar estimaciones en caso de que existan parámetros que muestran variabilidad.

Al hilo de lo anteriormente expuesto afloran tres nuevos conceptos:

- *Ciber-riesgos.*
- *Ciber-amenazas.*
- *Vulnerabilidades en sistemas de control industrial.*

Estas definiciones vienen a proporcionar ayuda para conseguir entender y posteriormente evaluar los riesgos (mediante cualquiera de los métodos existentes), facilitando así la toma de decisiones en el ámbito de la ciberseguridad de los sistemas de control industrial involucrados en infraestructuras críticas.

3.2.6.1. Ciber-riesgos

Los ciber-riesgos son los compromisos a los que una entidad, organismo o particular se encuentra expuesto, y cuyas causas provienen del uso y aplicación de las TI. Por consiguiente, estos se encuentran de manera

emergentes en el área de las TO por la ya ampliamente detallada interconexión en la industria 4.0, y como consecuencia de la convergencia entre TI y TO.

El ciber-riesgo representa una combinación de diferentes peligros (asumibles o no) cuya materialización pudiera causar daños en elementos intangibles (datos, alojamientos web, información, conectividad, propiedad intelectual) o elementos tangibles como pueden ser los productos resultantes en entornos operacionales. Del mismo modo estos daños pueden ser ocasionados a terceras partes implicadas, siendo de especial mención todos aquellos ocasionados a IC, los cuales pueden incurrir en catástrofes, personales, económicas, sociales e incluso medioambientales [Ley PIC, 2011].

Para entender la escalabilidad del nivel del riesgo que se posee en un determinado espacio temporal, la Figura 13 viene a representar el diseño de una matriz de riesgo, la cual involucra directamente dos parámetros para su evaluación: la probabilidad de que se materialice el evento y el impacto repercutido por el suceso, asociando un valor numérico a la relación [Mantha B., 2020].

La numeración y valores existentes en la matriz de riesgo, concretamente cada horquilla de probabilidad, lleva asociado un valor que se corresponde, al igual que el impacto, con el producto cartesiano resultante de:

$$Probabilidad = \{\, 1(0\% - 20\%), 2(20\% - 40\%), 3(40\% - 60\%), 4(60\% - 80\%), 5(80\% - 100\%)\}$$ Expresión (1)

$$Impacto = \{\, 1(Insignificante), 2(Menor), 3(Moderado), 4(Alto), 5(\ Muy\ Alto)\}$$ Expresión (2)

Probabilidad	(0%-20%)	(20%-40%)	(40%-60%)	(60%-80%)	(80%-100%)
Impacto	Insignificante	Menor	Moderado	Alto	Muy Alto
$\boldsymbol{A} * \boldsymbol{B}$	1	2	3	4	5

Expresión (3)

$$Probabilidad * Impacto = \left\{ \begin{array}{c} (\text{insignificante, Raro}), (\text{Insignificante, Improbable}), (\text{Insignificante, Posible}), (\text{Insignificante, Probable}), \\ (\text{Insignificante, Casi Seguro}), \\ (\text{Menor, Raro}), (\text{Menor, Improbable}), (\text{Menor, Posible}), (\text{Menor, Probable}), (\text{Menor, Casi Seguro}), \\ (\text{Moderado, Raro}), (\text{Moderado, Improbable}), (\text{IModerado, Posible}), (\text{IModerado, Probable}), (\text{Moderado, Casi Seguro}), \\ (\text{Alto, Raro}), (\text{Alto, Improbable}), (\text{Alto, Posible}), (\text{Alto, Probable}), (\text{Alto, Casi Seguro}), \\ (\text{Muy Alto, Raro}), (\text{Muy Alto, Improbable}), (\text{Muy Alto, Posible}), (\text{Muy Alto, Probable}), (\text{Muy Alto, Casi Seguro}) \end{array} \right\}$$

$$Probabilidad * Impacto = \{1, 2,3,4,5), (2,4,6,8,10), (3,6,9,12,15), (4,8,12,16,20), (5,10,15,20,25)\}$$

Expresión (4)

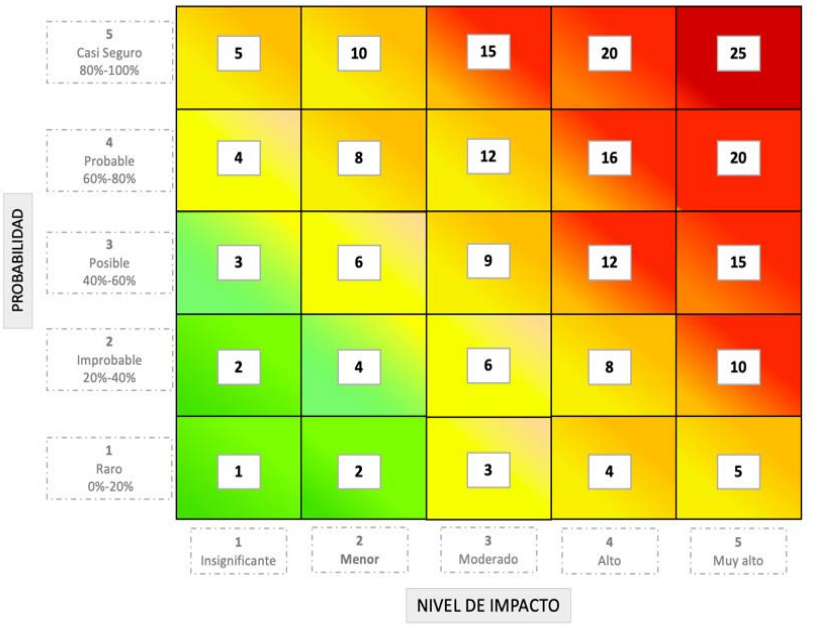


Figura 13: Matriz de riesgos.

Como complemento a la evaluación del ciber-riesgo y para su correcta estimación, se hace necesario el uso de ciertas métricas asociadas, herramientas para la validación de los datos obtenidos, así como los valores del tiempo de exposición y nivel del impacto y probabilidad de suceso. Para el desarrollo del cálculo numérico del nivel de riesgo se tienen en cuenta diversas variaciones de este riesgo, cada una de ellas dependiente de parámetros diferenciadores como son: tiempo de exposición, antigüedad de la vulnerabilidad y nivel de clasificación procedente del CVSS-SIG[44] (Common Vulnerability Scoring System*)* [URL- 23, 2021].

Por consiguiente, las estrategias a llevar a cabo para la evaluación de riesgos pasan por definir claramente las siguientes métricas:

[44] Se trata de un sistema de puntuación diseñado para proveer un método abierto y estándar que permite estimar el impacto derivado de vulnerabilidades identificadas en Tecnologías de Información, es decir, contribuye a cuantificar la severidad que pueden representar dichas vulnerabilidades.

- **Riesgo Real**

$$Riesgo = \frac{CVSS\ métrica\ de\ Impacto}{CVSS\ probabilidad\ de\ Impacto} * (t)\ \text{(Malware rango del Exploit)}$$ Expresión (5)

- **Riesgo temporal añadido**

$$Riesgo = \sqrt{t} * \frac{(1 + VA + C + I + D)}{(CA + Au)^2}$$ Expresión (6)

- **Riesgo temporal**

$$Riesgo = \sqrt{t} * \frac{(VA + C + I + D)^!}{(CA + Au)^2}$$ Expresión (7)

Donde (t) se corresponde con la probabilidad basada en el tiempo, y representa el número de días transcurridos desde que la vulnerabilidad se hizo pública. La puntuación global aumenta con el número de días. Los valores CVSS se refieren a los distintos vectores de componentes básicos de la versión 2 del CVSS, que se desglosa en 6 métricas base:

- *Vector de Acceso (**VA**).*
- *Complejidad de Acceso (**CA**).*
- *Autenticación Requerida (**Au**).*
- *Impacto de Confidencialidad (**C**).*
- *Impacto de Integridad (**I**).*
- *Impacto de Disponibilidad (**D**).*

El Instituto Nacional de Estándares y Tecnología (National Institute of Standards and Technology, NIST, por sus siglas en inglés) dispone de una herramienta de acceso libre, la cual facilita la posibilidad de obtener la puntuación de una vulnerabilidad en función a la valoración de los

parámetros de las métricas base especificadas anteriormente [URL- 24, 2021].

```
// Ecuación utilizada para el cálculo de la puntuación base CVSS
// CVSS Ecuación para el cálculo de la puntuación básica
BaseScore = (.6*Impact +.4*Exploitability-1.5)*f(Impact)
Impact = 10.41 * (1 - (1 - ConfImpact) * (1 - IntegImpact) * (1 -
AvailImpact))
Exploitability = 20 * AccessComplexity * Authentication * AccessVector
f(Impact) = 0 if Impact=0; 1.176 otherwise
AccessComplexity = case AccessComplexity of
                        high:   0.35
                        medium: 0.61
                        low:    0.71
Authentication   = case Authentication of
                        Requires no authentication:
0.704
                        Requires single instance of authentication:
0.56
                        Requires multiple instances of authentication:
0.45
AccessVector     = case AccessVector of
                        Requires local access:    0.395
                        Local Network accessible: 0.646
                        Network accessible:       1
ConfImpact       = case ConfidentialityImpact of
                        none:             0
                        partial:          0.275
                        complete:         0.660
IntegImpact      = case IntegrityImpact of
                        none:             0
                        partial:          0.275
                        complete:         0.660
AvailImpact      = case AvailabilityImpact of
                        none:             0
                        partial:          0.275
                        complete:         0.660
//CVSS Temporal Equation
TemporalScore = BaseScore
              * Exploitability
              * RemediationLevel
              * ReportConfidence
Exploitability   = case Exploitability of
                        unproven:             0.85
                        proof-of-concept:     0.9
                        functional:           0.95
                        high:                 1.00
                        not defined           1.00
RemediationLevel = case RemediationLevel of
                        official-fix:         0.87
                        temporary-fix:        0.90
                        workaround:           0.95
                        unavailable:          1.00
                        not defined           1.00
ReportConfidence = case ReportConfidence of
                        unconfirmed:          0.90
                        uncorroborated:       0.95
                        confirmed:            1.00
                        not defined           1.00
//CVSS Environmental Equation
EnvironmentalScore = (AdjustedTemporal
                        + (10 - AdjustedTemporal)
                        * CollateralDamagePotential)
                        * TargetDistribution
AdjustedTemporal = TemporalScore recomputed with the Impact sub-
equation replaced with the following AdjustedImpact equation.
```

```
AdjustedImpact = Min(10,
                     10.41 * (1 -
                                 (1 - ConfImpact  * ConfReq)
                                * (1 - IntegImpact * IntegReq)
                                * (1 - AvailImpact * AvailReq)))
CollateralDamagePotential = case CollateralDamagePotential of
                                 none:            0
                                 low:             0.1
                                 low-medium:      0.3
                                 medium-high:     0.4
                                 high:            0.5
                                 not defined:     0
TargetDistribution        = case TargetDistribution of
                                 none:            0
                                 low:             0.25
                                 medium:          0.75
                                 high:            1.00
                                 not defined:     1.00
ConfReq       = case ConfidentialityImpact of
                         Low:              0.5
                         Medium:           1
                         High:             1.51
                         Not defined       1
IntegReq      = case IntegrityImpact of
                         Low:              0.5
                         Medium:           1
                         High:             1.51
                         Not defined       1
AvailReq      = case AvailabilityImpact of
                         Low:              0.5
                         Medium:           1
                         High:             1.51
                         Not defined       1
```

Script 2: Definición algorítmica para la obtención de la puntuación base en CVSS.

```
//Árbol de decisión de la puntuación global del NVD CVSS
//La puntuación global del CVSS es parte del NVD y no forma parte del
estándar CVSS.
(Calculate OverallScore)
                |
                \/
<BaseScore Defined?>--No--> [OverallScore = "Not Defined"] -----
|
                |
|
                |
|
               Yes
|
                |
|
                \/
|
    [OverallScore = BaseScore]
|
                |
|
                |
|
                \/
|
<EnvironmentalScore Defined?> --Yes--> [OverallScore =
| EnvironmentalScore] ----------------------------------------
```

```
|                                                          |
|                                                          |
                  No
|
                  |
|
                  |
|
                  \/
|
<TemporalScore Defined?>--Yes-->[OverallScore = TemporalScore] -
                  |
|
                  |
|
                  No
|
                  |
|
                  |
|
                  \/
|                   (Return OverallScore) <-----------------------
```

Script 3: Árbol de decisión para la obtención de la puntuación global del NVD CVSS.

Los Scripts 2 y 3 representan la definición algorítmica de como internamente CVSS calcula los valores para la obtención de la puntuación base y global del NVD, respectivamente.

- **Riesgo ponderado.**

  El modelo de riesgo ponderado se basa principalmente en los datos de los activos y los tipos de vulnerabilidad. Hace hincapié en los siguientes factores:

  - *Gravedad de la vulnerabilidad, que oscila entre los valores 1 y 10.*
  - *Número de instancias de vulnerabilidad.*
  - *Tipo de activo, como un ordenador, un enrutador o un punto de acceso inalámbrico (WAP).*
  - *Número y tipos de servicios en el activo.*
  - *El nivel de importancia o peso que se asigna a un sitio al configurarlo (por ejemplo, bajo, alto).*

- **Riesgo PCI ASV[45]**.

Esta estrategia designa una puntuación basada en la norma de seguridad de datos del sector de las tarjetas de pago. PCI DSS enumera doce requisitos para el cumplimiento de la metodología. Entre uno de los requisitos para la evaluación de riesgos se define la *"Categorización de Vulnerabilidades"* la cual viene a aportar asistencia para la priorización de las medidas de solución y mitigación de los problemas identificados. Los proveedores de escaneo aprobados (ASV) deben asignar un nivel de gravedad a cada vulnerabilidad identificada (1 = gravedad más baja, 5 = gravedad más alta) y deben utilizar dos herramientas para categorizar y clasificar las vulnerabilidades y determinar el cumplimiento del escaneo:

- El Sistema de Puntuación de Vulnerabilidad Común (CVSS) versión 2.0.
- La Base de Datos de Vulnerabilidad Nacional (National Vulnerability Database, NVB, por sus siglas en inglés).

Cualquier vulnerabilidad con una puntuación base del CVSS de *4,0 o superior* dará lugar a un escaneo no conforme [Roldán G., 2017].

De igual manera, es importante resaltar que la propia ausencia de ciertas medidas correctivas actuantes sobre los propios factores de riesgo, deben ser consideradas como vulnerabilidades propias del entorno-sistema y que dada su importancia, se enumeran a continuación:

1. *Diversidad de culturas en materia de ciberseguridad del personal técnico.*
2. *Carencia en concienciación y formación.*

[45] PCI ASV hace referencia el requisito 11.2.2 de los Requisitos de la Norma de Seguridad de Datos (Data Security Standard, DSS) de la Industria de las Tarjetas de Pago (Payment Card Industry, PCI) y los Procedimientos de Evaluación de Seguridad que exigen escaneos externos trimestrales de vulnerabilidades, que debe llevar a cabo (o validar) un Proveedor de Escaneos Aprobado (Approved Scanning Vendor, ASV).

3. *Existencia de una falsa seguridad por parte de los propios fabricantes de instrumentación industrial.*
4. *Carencia de documentación procedimental y comunicaciones incorrectamente gestionadas.*
5. *Excesivos periodos de los ciclos de vida de los dispositivos industriales. Uso de sistemas operativos obsoletos y carentes de coberturas técnicas*.

A través de la Figura 14, se muestran todos aquellos sistemas operativos que Microsoft ha creado. Se hallan ordenados por orden cronológico de aparición.

Como ha quedado constatado en esta sección, existe una pluralidad de herramientas y metodologías a aplicar para el cálculo del riesgo que se ostenta y que se está dispuesto a asumir dentro de un entorno operacional.

SICERCAI ha sido diseñado para poder aplicar el sistema CVSS para una evaluación previa de un posible impacto ante situación de riesgo de un sistema, otorgando alta capacidad de prevención y resiliencia.

Figura 14: Representación cronológica de los sistemas operativos de TI, especificando los que conviven en la actualidad en los entornos de las TO.

3.2.6.2. Ciber-amenazas

Para poder comprender el concepto de ciber-amenaza se debe definir en primera instancia el concepto de amenaza, quedando encuadrada ésta dentro de "*la posibilidad de la materialización de cualquier tipo de evento o acción, capaz de producir un daño, ya sea de naturaleza material o inmaterial, sobre los elementos de un sistema".* Ésta engloba daños a nivel físico de funcionalidad e incluso de información. Por ende, ciber-amenaza corresponde a la materialización de estas acciones a través de "*el uso de la red, teléfonos móviles u otras tecnologías telemáticas, llevando a cabo la ejecución de una amenaza*" [URL- 25, 2021].

Estas ciber-amenazas que afectan a los sistemas de las TO, pueden proceder de acciones de carácter intencionado o no intencionado.

Las acciones no intencionadas abarcan a todas las que no afectan de una manera concreta a los sistemas de control y automatización, de ahí que se puedan ver afectados. Esta carencia de intencionalidad, implica a vulnerabilidades que en un principio son controlables.

Este tipo de amenazas a su vez se subdividen en cuatro grandes grupos: fallos de *safety, fallos en la equipación, desastres medioambientales y errores humanos.*

- Los fallos correspondientes al concepto de safety abarcan las problemáticas inherentes a los sistemas de protección de los equipos de instrumentación (PLC, sensores, actuadores, etc.) como de los operarios encargados de su manejo. Estos fallos afectan directamente al funcionamiento, pudiendo provocar deterioros en los sistemas de control, incluido el propio proceso industrial.
- Los fallos en la equipación van desde un error en las memorias de los dispositivos (disrupción en memoria principal de un PLC, desbordamiento de la memoria de un SCADA, etc.), hasta la

ruptura de cualquier elemento electrónico (fuentes de alimentación, interfaces de comunicación de un dispositivo remoto, etc.).

- Los desastres medioambientales engloban todos aquellos sucesos no controlables y de consecuencias catastróficas. Esta problemática se origina en fenómenos naturales adversos de índole incontrolable (terremotos, maremotos, etc.).
- Los errores humanos abarcan aquellos cuyo origen son meros descuidos o dejadez por falta de cultura en ciberseguridad (uso de medios personales como discos duros portátiles en entornos industriales y equipos conectados en la red corporativa).

Con respecto a las amenazas de carácter intencionado, estas involucran a todas aquellas acciones que de manera clara se dirigen contra los sistemas de control industrial, encuadrándose en empleados descontentos, pequeños grupos de hacktivismo[46], espionaje industrial, grupos criminales, terroristas y servicios de inteligencia extranjeros.

- Los empleados descontentos suponen un origen para la amenaza en las TIO de peculiaridades importantes para estos sistemas por su amplio conocimiento de las estructuras en las que se encuentran desarrollando sus labores diarias, de las configuraciones específicas de los sistemas críticos etc. Sobre este apartado surge la figura del denominado "*insider*" [URL- 26, 2017], la cual se hace eco de la existencia de una amenaza interna, de origen humano y motivada por aspectos tan notables como son:

[46] El término *hacktivismo* nace de la unión de dos palabras: *hacker* y activismo. Hace referencia al uso de la tecnología y de Internet de forma no violenta, normalmente para reivindicar posturas políticas o sociales.

- *Económicas,* cuya motivación está basada en la posibilidad de obtener dinero por las acciones a realizar.
- *Venganza*, sustentada por un descontento por parte del atacante, dimanante de un despido, falta de motivación, etc.
- *Distracción*, como acción de desvío de la atención por parte de los encargados de la ciberseguridad industrial, para llevar a cabo acciones mayores.
- *Desconocimiento*, probablemente originados por falta de cultura formativa en materia de ciberseguridad.
- *Espionaje industrial* sustentado por empresas de la competencia en el sector que intente materializar algún tipo de soborno.

- Los englobados dentro de hacktivismo activo son aquellos individuos que como consecuencia de la persecución de un afán de notoriedad individual causan daños. Estos daños pueden ser catalogados como daños colaterales resultantes de la acción de la obtención de su nivel de reputación.
- El espionaje industrial, en este ámbito se ven incrementadas las amenazas de esta categoría, cuyo objetivo es acceder a datos concretos e informaciones sensibles con los que ganar competitividad, visibilidad y presencia en el sector, además de obtener una cuota de mercado en base al desarrollo de productos y campañas derivados de otros sustraídos.
- Los grupos de criminales actúan bajo su propia definición, empleando chantajes para la obtención de dinero a cambio de la no revelación de información sensible operacional o de negocio.
- El terrorismo aplicado a los entornos de automatización industrial implica una amenaza física directa a las infraestructuras, siendo su finalidad la destrucción. Se debe resaltar en esta subsección, como ya quedó demostrado a través del proyecto "Aurora" [URL-27, 2007], llevado a cabo

en las instalaciones del Gobierno de Estados Unidos de América (Estado de Idaho), que, mediante un ciberataque a nivel lógico, se puede llegar a causar una destrucción física de un artefacto. La documentación completa de este proyecto, puede ser consultada en el repositorio documental habilitado al efecto [URL- 00, 2020].

- Por último, los servicios de inteligencia de estados extranjeros se nutren de información la cual puede llegar a facilitar la materialización de un ciberataque a gran escala. Esta área, en la actualidad, está definiendo nuevos escenario para el nuevo concepto de ciberguerra [URL- 28, 2020].

Tras la visión ampliada de la categorización del tipo y modelos de ciber-amenazas a las que se encuentran expuestos los sistemas de control industrial, el siguiente paso se corresponde con cómo prevenir este tipo de amenazas.

Aunque no existe un método infalible, se debe permanecer prevenidos ante las posibles amenazas. Como consecuencia de la ejecución de un SGCI se deben realizar planes de concienciación de equipo, instruyendo en el uso seguro de las tecnologías a su alcance mediante campañas de formación y prevención, involucrando a todo el personal implicado. Además, establecer un canal de información, haciendo partícipe al empleado de las posibles amenazas mediante circulares informativas (prevención), correos electrónicos o cualquier otro medio a su alcance, logrando así mejorar la sensibilidad ante estos temas y poner en guardia al personal ante situaciones de riesgo no previstas.

Se debe poner todo el esfuerzo en la creación y diseño de nuevas arquitecturas de pruebas que permitan la recreación de los entornos desplegados en la parte de operación como de las TI, para poder detectar las vulnerabilidades que se encuentran expuestos los sistemas, sus posibles

riesgos y niveles de asunción de los mismos, potenciando así la capacidad en ciberseguridad y ciber-resiliencia (SICERCAI).

No existe una solución, o una receta mágica para evitar una amenaza, pero sí se pueden minimizar, aplicando la prevención como norma general.

3.2.6.3. Vulnerabilidades en sistemas de control industrial

Las vulnerabilidades emergentes y descubiertas en los sistemas de control industrial han sufrido un gran aumento la última década. Concretamente, el hito que marcó este punto de inflexión fue la aparición del malware[47] Stuxnet en el año 2010 [Sembiring Z., 2020].

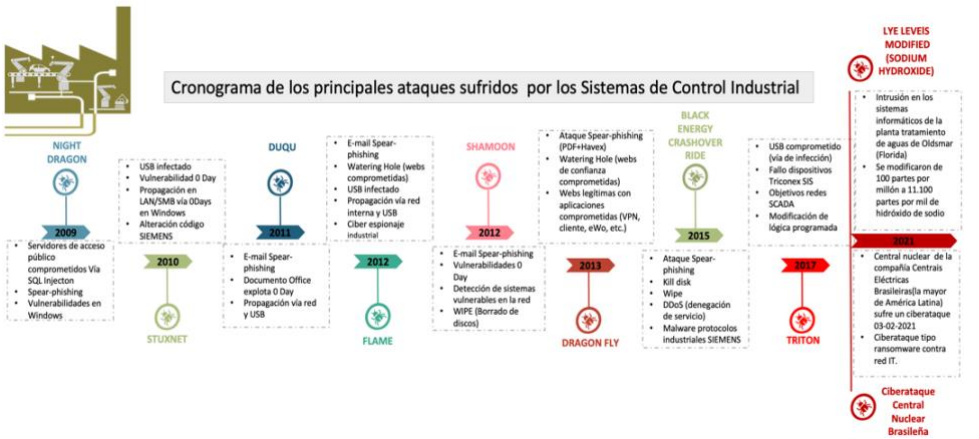


Figura 15: Cronograma de los principales ataques dirigidos a SCAI.

La Figura 15, muestra un cronograma de los principales ataques sufridos por los sistemas de control industrial a lo largo de la última década.

Este aumento notorio desde el año 2010 no viene a proporcionar información relevante sobre la inexistencia previa de vulnerabilidades en los SCI, anteriormente a esa fecha; lo verdaderamente esclarecedor de esos datos corresponde al interés suscitado por la comunidad de la ciberseguridad

[47] Malware es un término general para referirse a cualquier tipo de software malicioso, cuyo fin y diseño es infiltrarse en dispositivos sin su conocimiento.

en materia de vulnerabilidades de esos sistemas y la problemática asociada y extrapolada a las infraestructuras críticas de los países.

Anteriormente al año 2010 hubo otros incidentes, los cuales tuvieron un carácter relevante por su naturaleza pero no así por el impacto desencadenado. Éstos fueron:

- *Planta tratamiento de aguas en Maroochy Shire (Australia), año 2000.* Fueron vertidos más de 2 millones de litros de aguas residuales en el paraje natural del condado de Maroochy (Australia). Las consecuencias del vertido impactaron directamente en un elevado número de pérdidas de vidas de animales salvajes. La acción fue llevada a cabo por un empleado de la empresa de manera intencionada [URL- 33, 2017].
- *Central nuclear Davis Besse (OHIO, EEUU), año 2003.* La central nuclear sufrió una infección por el gusano "Slammer[48]", afectando a varios sistemas de monitorización de la planta. El acceso se propició a través de un enlace directo y externo de un tercero. El parche que solventaba esa falla de seguridad se encontraba disponible desde varios meses antes del ataque [URL- 34, 2018].
- *Central nuclear de Browns Ferry (Alabama, EEUU), año 2006*. Se produjo un fallo en un PLC del desmineralizado por condensación y de las dos bombas de recirculación redundantes. Por tal motivo la central tuvo que ser llevada a una parada controlada para evitar males mayores. La causa fue un fallo técnico de los procesadores embebidos de los PLC y los

[48] El gusano Slammer se propagó a través de una vulnerabilidad de tipo *desbordamiento de buffer* en distintos productos de *Microsoft SQL Server* donde no se habían instalado el *Service Pack 3*. Slammer enviaba un paquete de aproximadamente 380 bytes al puerto 1434 UDP, los sistemas vulnerables y ya infectados, empezaban a enviar de manera inmediata este mismo paquete provocando un ataque DDoS o de denegación de servicios distribuido.

variadores de frecuencia que no soportaron el excesivo tráfico de red existente [URL- 35, 2006].

- *Sistema ferroviario de Lodz (Polonia), año 2008.* Durante ese año se produjeron una serie de descarrilamientos en la ciudad polaca de Lodz. Las causas fueron la capacidad de que un joven a través de un mando de radiofrecuencia fuese capaz de variar las agujas de cambio de vías. Realizó un estudio previo de trenes y rutas (fase de reconocimiento y preparación) [URL- 36, 2008].
- *Central nuclear Edwin I. Hatch (Georgia, EEUU), año 2008.* Se produjo una parada automática de la central nuclear durante 48 horas. Esto fue ocasionado por una actualización del software sobre el ordenador que controlaba la monitorización de los datos químicos y de diagnóstico asociados al sistema de control. Se produjo un reinicio que derivó en la falta de información momentánea de datos [URL- 37, 2008].

Como complemento a esta subsección se incluye el documento completo resultante del estudio realizado por el Centro de Ciberseguridad Industrial (CCI) sobre la evolución de la vulnerabilidades detectadas y clasificadas durante los años 2010 al 2020 [URL- 00, 2020].

La Tabla 10 recoge a modo de síntesis, varias vulnerabilidades del fabricante SIMENS, y a su vez de diferentes modelos de SACI, las cuales han sido reportadas por ICSA [URL- 29, 2021].

SIEMENS
ICSA-21-012-05 : Siemens SCALANCE X Products
ICSA-21-012-04 : Siemens Solid Edge
ICSA-21-012-03 : Siemens JT2Go and Teamcenter Visualization
ICSA-21-012-02 : Siemens SCALANCE X Switches
ICSA-20-343-10: Siemens LOGO! 8 BM
ICSA-20-343-09 : Siemens SIMATIC Controller Web Servers
ICSA-20-343-08 : Siemens Products using TightVNC

ICSA-20-343-07 : Siemens SICAM A8000 RTUs
ICSA-20-196-08: Siemens LOGO! Web Server

Tabla 10: Tabla resumen de las vulnerabilidades que afectan a productos SIEMENS, con direccionamiento directo a ICSA.

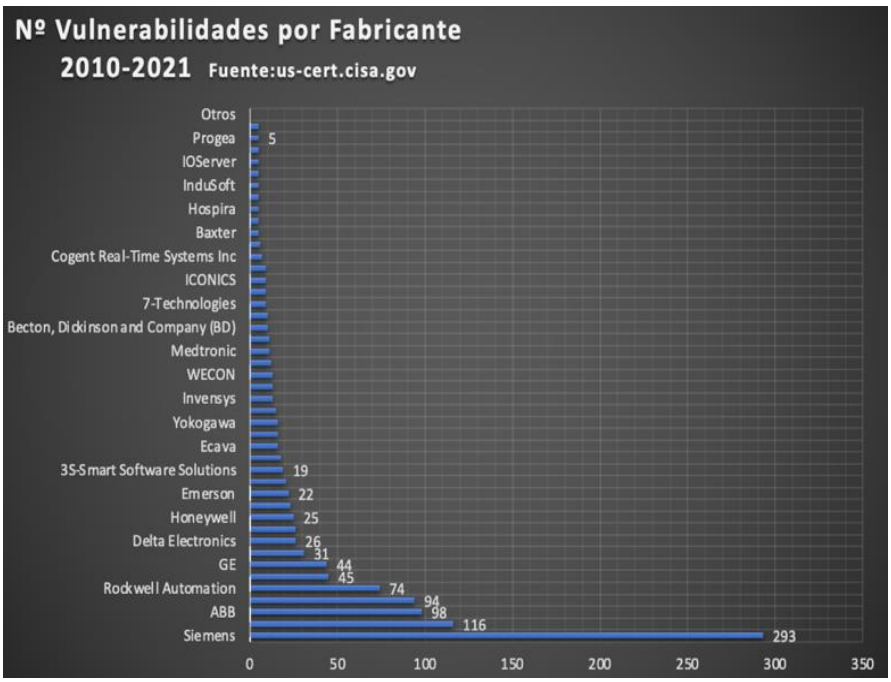


Figura 16: Gráfico resumen agrupando vulnerabilidades reportadas durante el periodo de estudio 2010 al 2020, agrupadas por fabricantes.

Como se puede observar en la Figura 16, se ha elaborado una gráfica correspondiente al número de vulnerabilidades existentes en varios tipos de dispositivos industriales agrupadas por fabricantes. El estudio realizado corresponde a un total de ***374 fabricantes*** diferentes, habiendo sido datadas ***1.573 vulnerabilidades***. Cada una de estas vulnerabilidades posee su correspondiente informe completo en el que se refleja la gravedad del CVSS, la evaluación del riesgo, los detalles técnicos, el listado completo de los productos afectados, y los procesos a realizar para su completa mitigación [URL- 29, 2021].

El listado completo del estudio llevado a cabo desde marzo del año 2010 hasta febrero de 2021, con las vulnerabilidades de los diferentes fabricantes formalmente documentadas, se encuentra ubicado en el

repositorio de documentación habilitado al efecto para su consulta [URL-30, 2021].

Estos tipos de vulnerabilidades pueden ser categorizadas de diversas maneras. En la presente Tesis, y siguiendo la línea optada desde un principio y en la que SICERCAI se ha sustentado para su creación y desarrollo, se sigue la categorización que realiza NIST, según su publicación NIST SP 800-82 (apartado 3.2.2) [URL-31, 2021]. Se establecen cuatro grandes categorías: vulnerabilidades de plataforma, de red, procedimentales y vulnerabilidades técnicas:

1. ***Vulnerabilidades de plataforma***

Estas agruparán a todas aquellas vulnerabilidades que se puedan hallar en los dispositivos, incluyéndose las de los centros de control y de las redes operacionales o de campo. A su vez, éstas estas pueden categorizarse en configuración de la plataforma, vulnerabilidades de hardware, vulnerabilidades del software y las existentes frente al malware.

En este tipo de vulnerabilidades quedan englobados los estados de equipos desactualizados con un escaso o desprovisto control de acceso, numerosos puertos de conexión físicos indebidamente protegidos, servicios habilitados en los equipos de manera innecesaria (gran exposición), uso de configuraciones por defecto, contraseñas por defecto y con inexistencia de una política adecuada (plazos de expiración, robustez y almacenamiento inseguro).

2. ***Vulnerabilidades de red***

Este tipo de vulnerabilidades engloban los problemas se seguridad relacionados con las comunicaciones industriales a nivel de flujo de comunicaciones como de arquitectura. Esta tipología se sub-divide a su vez en: vulnerabilidades de configuraciones de la red, vulnerabilidades inherentes del propio hardware de los componentes de la red,

vulnerabilidades por las carencias perimetrales de la red y de su monitorización y las vulnerabilidades de las propias comunicaciones.

Destacan entre ellas las asociadas a una carencia de segmentación de las redes. Como punto de desarrollo de buenas prácticas deben ponerse en práctica las recomendaciones establecidas en el estándar IEC 62443 en concreto su apartado *A.3.3.4.2,* en donde se detalla la división en los correspondientes segmentos de red y zonas (cinco niveles y DMZ o zona desmilitarizada [URL-32, 2019]).

3. ***Vulnerabilidades de procedimientos y despliegues***

Por último, y no por ello menos importantes, este tipo de vulnerabilidades afectan al marco de la gestión de la ciberseguridad de naturaleza procedimental y normativo. La ciberseguridad debe tener un rol claramente holístico[49], concepto creado en el año 1926 por Jan Christiaan Smuts, por el que se define que un sistema y sus propiedades, debe ser analizado como un todo de manera global e integrada, implicando las medidas a establecer en el área de la ciberseguridad a toda la organización al completo y desterrando el concepto de la funcionalidad global como la simple suma de sus partes.

Esta clasificación está caracterizada por una inexistencia de normas de seguridad previamente establecidas en la parte de las TO, estando las guías de buenas prácticas enfocadas para el área de las TI. De igual manera prácticamente no existen procesos de gestión de cambios ni de auditorías (internas o externas), motivadas estas últimas por la naturaleza sumamente peligrosa de la alta disponibilidad en los SCAI. A su vez destacan carencias en planes de formación y sensibilización desde los empleados en las TO hasta la

[49] El holismo puede ser definido como una visión global que parte del todo para captar sus componentes en contexto y sus interacciones entre estos y con el todo.

alta dirección. En muchas ocasiones no existe un inventario de activos, o si se constata su presencia, éste suele estar desactualizado.

4. ***Análisis de vulnerabilidades técnicas***

Este tipo de análisis en el entorno de las TO y de las TI es poco usual frente a la normalidad de su ejecución, tanto en frecuencia como en intensidad.

Todos los puntos expuestos en esta sección vienen a corroborar la importancia de tener correctamente establecido un SGCI. Por ese motivo, SICERCAI colabora aportando ventajas claras para ser considerado como parte de ese sistema de gestión de ciberseguridad industrial, proporcionando capacidad de análisis previo de los sistemas y arquitecturas a desplegar en la industria operacional.

3.2.7. Gestión del riesgo frente a los ciberataques

La clave para detectar, detener, interrumpir y recuperarse ante un ciberataque, pasa en primer lugar por comprender cuál es su ciclo de vida y así obtener la capacidad de desarrollar e implementar todas las operaciones necesarias, que garanticen el mayor grado de prevención y resiliencia, redundando estas acciones en una mayor protección de los sistemas.

A este ciclo de vida se le conoce como "*cadena de ataque*"(Cyber Kill Chain, CKC, por sus siglas en inglés) [Straub J., 2020], [Hutchins E., 2011].

Este concepto en su origen fue acuñado por organismos militares para especificar los pasos que usaba el *enemigo* a la hora de proceder a atacar un objetivo. De igual manera fue usado por analistas de la empresa aeroespacial y de seguridad global "Lockheed Martin Corporation[50]" como parte de un

[50] Con sede en Bethesda, Maryland, Lockheed Martin es una empresa aeroespacial y de seguridad global que emplea a aproximadamente 110.000 personas en todo el mundo y se dedica principalmente a la investigación, el diseño, el desarrollo, la fabricación, la integración y el mantenimiento de sistemas, productos y servicios de tecnología avanzada.

modelo para ayudar en la toma de decisiones en el momento de responder ante ciberataques e intrusiones de sus sistemas.

A modo de recordatorio y para profundización en su taxonomía, las siete etapas que componen la consumación de un ciberataque, se corresponden con:

1. *Reconocimiento.*
2. *Preparación.*
3. *Distribución.*
4. *Explotación.*
5. *Instalación.*
6. *Acciones de comando y control.*
7. *Acciones a ejercer sobre os objetivos* (ver Figura 7, sección 3.2.5).

Con el fin de prosperar y alcanzar el éxito desde un posicionamiento defensivo e intentar romper esa cadena de ejecución de un ciberataque en cada una de las diferentes etapas, se conciben las siguientes acciones posibles a llevar a cabo en cada una de ellas y a las que SICERCAI contribuye dada su arquitectura, viéndose implicado en varias de las etapas.

- **Reconocimiento**. Desde el punto de vista defensivo, tener capacidad de ser predictivo es importante, puesto que es la primera etapa del ataque dirigido. Por consiguiente, tener desplegado sistemas de análisis del tráfico de red y materializar una eficaz segmentación de redes en las TO se consideraría el primer escalón ante una defensa en profundidad.
- **Preparación**. En este punto y desde la perspectiva de la defensa, tener un buen conocimiento de los vectores de ataque a los que estamos expuestos suele ser la táctica más efectiva y duradera.
- **Distribución**. Si en esta etapa se posee la capacidad de interrupción, es la inicial y más importante para producir un bloqueo de la intrusión.

- **Explotación**. Aquí la importancia radica en evitarla mediante una buena política de modificación y personalización de todas aquellas configuraciones por defecto de los dispositivos.
- **Instalación**. Uso y ejecución de herramientas de seguridad a nivel endpoint (puntos finales de red, las cuales proporcionan e integran datos para análisis forense, permitiendo respuestas rápidas ante un evento de ciberseguridad).
- **Comando y control**. Probablemente, esta sería la última fase en la que se podría ostentar la capacidad de romper la cadena, bloqueando la ejecución del malware o amenaza persistente avanzada instalada (Advanced Persistent Threat, APT, por sus siglas en inglés).
- **Acciones**. Se debe considerar que cuanto mayor sea el tiempo de acceso total al sistema, mayor será el impacto. Por ello, desde el rol de defensor es primordial quebrar esta fase del ataque haciendo uso del análisis forense de los sistemas.

Dado que los entornos de las TO carecen de visibilidad, aplicar los controles de seguridad resulta difícil a la vez que complicado, y detectar las amenazas en tiempo real o incluso después del ciberataque se torna arduo. Por lo tanto, es importante prevenir y detectar dichos peligros antes de que se hagan con el control de los procesos operativos y de los servicios críticos.

Teniendo bien definidos todos y cada uno de los pasos así como sus posibles mitigaciones ante un potencial ciberataque, a la vez que se conoce el nivel de exposición de los sistemas TI y TO desplegados, se posee la capacidad de detener el intento de intrusión en cualquiera de sus fases, resultando así quebrada la secuencia del ataque.

Dada la importancia de la predicción (capacidad de anticiparse), frente a la resiliencia (capacidad de reponerse ante una eventualidad) en materia

de ciberseguridad en los SCI de infraestructuras críticas, se deben incorporar dispositivos que faciliten y ayuden a una predicción a nivel técnico.

Las tecnologías IIoT pueden ayudar en el mantenimiento predictivo, optimizando las cadenas de suministro y otras características de ciberseguridad. Sin embargo, la mayoría de los dispositivos no están diseñados con la ciberseguridad como principal prioridad. Como consecuencia, estos dispositivos pueden colaborar a exponer el entorno industrial a una amplia gama de amenazas cibernéticas.

3.2.7.1. Inventariado de activos (TI-TO)

Cada vez es mayor la concienciación existente en las organizaciones para poder conseguir un nivel alto de ciberseguridad en sus entornos, o al menos aceptable y asumible. Pero en contrapartida sigue existiendo un problema en la sombra que acecha a la mayoría de las organizaciones, y es la carencia de conocimiento del número total de activos existentes. Poder disponer de un inventario actualizado de los elementos desplegados en el entorno a evaluar constituye el primer paso para la definición de un eficiente SGCI (Figura 6 de la sección 3.2.4.1,). En este tipo de listados deben estar añadidos todos aquellos actores intervinientes, y que a su vez posean valor en el desarrollo de la actividad diaria dentro de la organización (recursos técnicos, software, personal, comunicaciones, instalaciones, etc.).

Este enfoque debe poseer un carácter dinámico, porque como ha quedado reflejado con anterioridad en diversas ocasiones, las amenazas a la que se encuentran expuestos los sistemas de control industrial evolucionan y se especializan constantemente. Por consiguiente ostentan una naturaleza sofisticada y acorde a la convergencia entre las TI y TO.

Como se puede apreciar en las Figuras 17 (a) y (b), la definición de un inventario correcto y eficaz de activos consta de dos etapas principales: creación del inventario de activos y gestión del inventario de activos.

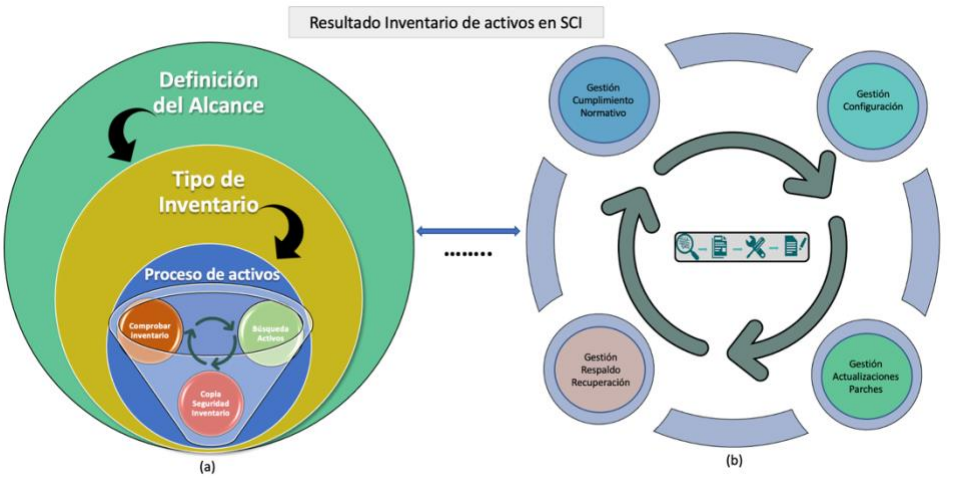


Figura 17: Procesos implicados en la ejecución de un inventario de activos (a) y (b).

A. ***Creación del inventario.*** Disponer de un inventario actualizado y que refleje la realidad de lo que se posee en las áreas de producción no aporta nada más que ventajas, puesto que viene a ofrecer capacidad de gestión de las vulnerabilidades, y repercute en una posible respuesta ante un evento imprevisto de ciberseguridad de manera rápida y eficiente (se posee en todo momento una fotografía real de las versiones de los SO y de firmwares). De igual manera contribuirá una veloz identificación de fallos a nivel operativo redundando en un incremento de la eficiencia de medios y sistemas.

Como premisa para la creación de un inventario de activos en los SCI, se debe definir el alcance, tener claro el tipo de inventario que se quiere realizar, ejecutar la búsqueda y mantener actualizado el catálogo creado.

- ***Alcance.*** Esta etapa no implica la limitación numérica de la cantidad de dispositivos a catalogar, que evidentemente deben estar contenidos

absolutamente todos, sino a delimitar la cantidad de información a recopilar de cada uno de ellos. Una correcta definición del alcance redundará en una protección eficiente a la hora de gestionar sus vulnerabilidades (fases implicadas "*gestión de configuraciones-actualizaciones-parches*").

- ***Tipo de inventario.*** Para la correcta elaboración del alcance existen varias modalidades de ejecución. Se puede realizar de manera automática, estando implicadas herramientas especializadas para tal fin, recolectando información de los dispositivos existentes de manera completamente desatendida. En este aspecto, es importante destacar que debe diferenciarse el ámbito de aplicación para este tipo de soluciones, teniendo muy en cuenta si es para un escáner activo (recomendado para entorno de las TI) o por lo contario un escaneo pasivo (recomendado para entorno de las TO, por su escasa intrusión).

Otra modalidad es realizar el escaneo de forma manual. En ella se encuentran implicadas una o varias personas de la organización, las cuales están encargadas de recopilar los datos de todos y cada uno de los dispositivos. Esta acción requiere de una metodología muy estricta por la dificultad que ello representa, que en ocasiones se torna inacabable por el elevadísimo número de dispositivos obrantes. En contrapartida, es una buena conducta por su escaso índice de peligrosidad. Se recomienda esta variante del tipo de escaneo en entornos de pocos elementos.

Por último, sería aplicar una variante mixta. Esta forma permite la realización de un inventariado completo, aprovechando las ventajas de las dos metodologías anteriores. Esta variante se recomienda para un número medio de activos.

Como ya se ha mencionado, los inventarios automáticos pueden ser catalogados según su naturaleza como:

- ***Activos***. Estos requieren una intervención directa sobre el elemento a inventariar o incluso contra la red de comunicaciones que lo soporta. Suelen ser llevados a cabo con el apoyo de algún *script*, cuya misión es la ejecución de una serie de comandos que pueden llegar a repercutir negativamente causando un impacto desastroso en redes industriales (esta redes soportan menores tiempos de latencia que las redes TI). Esta latencia concretamente se refiere al tiempo de retraso implicado directamente en la transmisión de datos a través de la red. Como quedó descrito al principio de este capítulo, la disponibilidad es el bien crítico a proteger en el área de las TO, frente a la integridad que corresponde en las TI.
- ***Pasivos.*** Por el contrario, cuando el inventario es de naturaleza pasiva, no se ejecutan acciones intrusivas, sino que se ejecuta a través de un análisis de tráfico de red o ficheros de configuración de los activos. Existen soluciones que su base es el análisis de red duplicado de manera física. A esta acción se la conoce como "*Port Mirroring*" o puerto espejo, y corresponde a la capacidad que tienen ciertos switches[51] para poder replicar de manera transparente el tráfico recibido por una de sus entradas.

B. ***Gestión del inventario***. Tras la ejecución del correspondiente inventario de activos, éste debe permanecer actualizado, modificándolo cada vez que se produzca alguna alteración (bien por eliminación/sustitución o agregación de activos), y manteniendo, a su vez, copias de seguridad de los inventarios de los activos (fases implicadas, "*Gestión Respaldo-*

[51] El switch es un dispositivo que se utiliza para conectar equipos en red, formando una red de área local (LAN) y se encargan de la interconexión de dispositivos y de equipos dentro de una misma red, siguiendo las especificaciones técnicas del estándar Ethernet.

Recuperación"). Disponer de un inventario actualizado permite disponer de una fotografía real de todos los activos que forman parte de un proceso. Mantener un control de acceso restringido a un inventario debe ser monitorizado y limitado única y exclusivamente al personal debidamente acreditado y autorizado. Esto evitará posibles modificaciones potencialmente peligrosas para la organización.

ACTIVO		DESCRIPCIÓN	ELEMENTOS
Hardware		Equipación física implicados en el proceso industrial	PLC, RTU, Servidores, IED, HMI
Software		Aplicaciones utilizas para la gestión de los procesos	SCADA, Sistemas Operativos, Firmware, herramientas de ingeniería y desarrollo
Personal		Personal partícipe en todos y cada uno de los estamentos de la organización	Fijos, subcontratados, proveedores cadena suministro
Información		Datos generados, transmitidos y eliminados (independientemente del formato y soporte)	Bases de datos, documentación de operación, manuales, guías de buenas prácticas
Red		Elementos de conectividad de red	Routers, Switches, cortafuegos
Equipación Auxiliar		anteriores apartados	verificación de identidades
Instalaciones		Infraestructuras en las que se alojan los equipos	Oficinas, áreas de producción, edificios

Tabla 11: Ejemplo ilustrativo de clasificación de activos. (modificada de la fuente original: INCIBE-CERT).

Por último y no menos importante, se debe tener en cuenta en el momento de la definición de una correcta ejecución y mantenimiento de inventarios, el cumplimiento normativo existente al respecto (interno de la organización y externo normativo). Esta normativa interna tendrá en cuenta los tiempos de paradas programadas para la realización de tales fines, duración y espacio temporal de las mismas, frecuencia operativa, áreas implicadas, etc.

De igual manera la normativa externa, corresponderá a la situación que afecte a entorno de producción por la naturaleza propia como IC, puesto que, a modo de ejemplo, el sector nuclear en este ámbito, se rige por normas muy diferentes al del sector transporte. Para poder ejecutar una correcta gestión de los activos existentes en la organización, es muy importante, poseer una

visión sobre la naturaleza de los mismos. A modo de ejemplo la Tabla 11 en la que se refleja una posible clasificación de los activos.

3.2.7.2. Problemática asociada a la ciberseguridad

Seguridad Tecnologías Información (TI)		Seguridad Tecnologías Operación (TO)
Confidencialidad Integridad | Disponibilidad		**Disponibilidad** Integridad | Confidencialidad
Alta permisibilidad en altas latencias	**Tiempos de respuesta**	**Baja permisibilidad** en altas latencias
2/3 años, gran núm de proveedores	**Ciclo de vida**	**10/20** años proveedores muy específicos y sectoriales
Habitual e integrado en el proceso	**Evaluación del riesgo**	Realizado **si es obligatorio**
Común, fácil, definidas y automatizadas	**Antivirus/parches**	**Poco habitual**, complejo sin políticas definidas
Utilización de metodologías estándares	**Testeo y Auditorias**	**Inexistencia** de metodologías estándar
Fácil despliegue y comunmente obligatorias	**Administración de Vulnerabilidades**	**Poco habitual**, sin actuaciones forenses a penas

Figura 18: Tabla comparativa de las necesidades y peculiaridades de las TI y TO.

Para complementar esta sección, y tras haber fijado un recorrido claro y dirigido de todos aquellos actores implicados en los sistemas de control industrial y su ciberseguridad aplicada, han sido involucrados en los SACI todos los nuevos paradigmas emergentes. Esto ha sido consecuencia directa del avance imparable de la convergencia entre las tecnologías de la información y de la operación. De igual manera se ha descrito su evolución respecto a su madurez (en ámbitos de ciberseguridad) y se han detallado acciones a ejecutar para destacar la problemática asociada a la convergencia entre las TI y las TO.

Los datos detallados en este capítulo pueden ser considerados verdaderamente reveladores por las complicidades y dependencias extraídas de la CTIO.

Han sido descritos los nuevos escenarios a los que los SCI se encuentran inmersos por sus exposiciones a los nuevos riesgos y amenazas que acechan a las organizaciones. Por este motivo, en paralelo surge una problemática asociada a la ciberseguridad de los entornos industriales, con dos líneas

claramente definidas: la que involucra únicamente a las organizaciones y la que implica a la sociedad en general y a sus intereses en particular. A modo de resumen de lo explicado hasta el momento, por la alta dependencia de las TO en las TI, se plantea la primera disyuntiva que corresponde al tratamiento tan diferente en sus prioridades ante la ciberseguridad. En la Figura 18 se detallan las premisas diferenciadoras entre las TI y las TO con respecto al orden de prioridad en los pilares que sustentan la seguridad de ambas tecnologías (disponibilidad, integridad y confidencialidad).

De todo ello surge la formulación de varias preguntas encaminadas a alcanzar y vislumbrar la implicación que puede llegar a tener el ámbito cibernético (lógica computacional) con el área física, sobre todo cuando ha sido explicado que, dada la naturaleza intrínseca de los sistemas industriales, creados para una larga duración en el tiempo por su robustez, están diseñados para periodos de funcionalidad superior a 20 años en entornos verdaderamente hostiles (altas temperaturas, frío-calor extremos, radioactividad, etc.) y completamente aislados. Pues bien, el gobierno de los Estados Unidos de América en el año 2007, en el Laboratorio Nacional de Idaho Falls (Idaho) [URL- 38, 2021] llevó a cabo un experimento denominado *"AURORA"* [URL- 39, 2007].

El objetivo de dicho experimento fue demostrar la importancia y repercusión que tenía la ciberseguridad (como concepto clásico) en las infraestructuras industriales, concretamente en el sector eléctrico.

El ciberataque controlado consistió básicamente en lo siguiente: a un motor diésel usado para la generación de energía eléctrica, que utilizaba el protocolo de comunicaciones MODBUS[52], desconectarlo de la red eléctrica de una manera intermitente, y durante el suficiente tiempo para que

[52] Modbus es un protocolo de comunicación abierto, utilizado para transmitir información a través de redes en serie entre dispositivos electrónicos.

perdiera los datos de sincronización de sus elementos de giro. En primera instancia fue aumentada la frecuencia por encima de la que operaba la red de suministro, haciendo saltar el sistema de frenado encargado de hacer bajar la frecuencia. Estos cambios hicieron fallar a los relés de control del sistema de frenado dañando sus partes mecánicas, produciendo fuertes sacudidas y, como consecuencia de ello, una explosión del propio generador unos minutos más tarde del comienzo de la disrupción.

Este ciberataque controlado supuso la demostración de que una irrupción a nivel lógico, repercutía directamente en el ámbito físico, por lo que se estaba ante la grandísima problemática que eso podría causar a la industria en general y a las IC en particular. El experimento fue clasificado como secreto[53] hasta el año 2014 por el Departamento de Seguridad Americano (Department Homeland Security, DHS, por sus siglas en inglés).

A raíz de este experimento, el paradigma de la protección de sistemas que estaban desplegados en infraestructuras críticas había cambiado radicalmente.

[53] La información clasificada es cualquier información o material respecto de la cual se decida que requiere protección contra su divulgación no autorizada y a la que se ha asignado, con las formalidades y requisitos previstos en la legislación, una clasificación de seguridad entendiéndose como información todo conocimiento que puede ser comunicado, presentado o almacenado en cualquier forma (www.cni.es).

La Figura 19 resume de manera gráfica las partes implicadas bajo un marco de protección cibernética en los SCI, las partes componentes en el Holismo aplicado a la ciberseguridad, siendo declarados estos conceptos en la Tabla 12.

Figura 19: Resumen de los procesos implicados en la definida cultura de la ciberseguridad.

Holismo aplicado a la ciberseguridad
• El holismo es un concepto creado en el año 1926 por Jan Christian Smuts
• Un sistema y sus propiedades se analizan como un todo
• De una manera global e integrada
• Se destierra el concepto de la funcionalidad global como la simple suma de sus partes

Tabla 12: Resumen del concepto de holismo aplicado a la ciberseguridad.

Por consiguiente, la ciberseguridad aplicada a los sistemas de control y por ende, a los existentes en las infraestructuras críticas, ostenta una importancia innata por hechos tan relevantes como los expuestos, y como consecuencia de los nuevos vectores de ataques surgidos por la convergencia de las TI y la TO.

Es importante resaltar, la existencia de un proceso gobernado desde el holismo. A este concepto en la actualidad se le conoce como Innovación holística, aplicada a la ciberseguridad de los SCI.

3.2.8. Tendencias y predicciones más significativas a nivel técnico y normativo en los SCI

Existe una tendencia conducente a que cada vez más organizaciones de desarrollo de actividades industriales realicen fuertes inversiones para incrementar la ciberseguridad y ciber-resiliencia de sus entornos o mejorar los que ya poseen. Con la creciente aparición de más amenazas, ya no solo las grandes empresas, sino también las pequeñas y medianas empresas, querrán mejorar la seguridad de sus entornos industriales para garantizar la continuidad de sus negocios.

Varios estudios arrojan cierta claridad sobre que la seguridad de los SCI se volverá más "convencional" con el paso del tiempo [URL- 40, 2021], pero la cuestión a plantearse realmente es la definición de "tiempo". Como se ha detallado en secciones anteriores, la relación que existe entre la ejecución de un suceso malicioso y su detección por parte de la organización transcurre una media de *274 días* según un informe elaborado por *"Sofistic Cybersecurity"* [URL- 41, 2021], situación que es inasumible en entornos de las TO de las infraestructuras críticas.

La proliferación de nuevas herramientas, tácticas y avances en las comunicaciones están poniendo bajo el punto de mira a los entornos operacionales cuyo fin es el de llevar a una ejecución exitosa la explotación de vulnerabilidades a las que se encuentran expuestos. Los ciberataques que reciben los entornos de las TO se multiplicarán en los próximos años, como consecuencia del aumento de la complejidad y selección más concreta de esos objetivos.

Como muestra de ello se detallan varias de las nuevas tendencias así como la explicación de su aplicación al sector de la industria y de las IC, siendo importante destacar la complejidad y sofisticación táctica y operativa de las mismas.

- Según un informe liberado por FortiGuard Labs (Fortinet), predice que *"...el uso de ciber-armas inteligentes alterará drásticamente la velocidad y la escala de futuros ataques"* [URL- 42, 2020]. El posible vector de intrusión no estará enfocado directamente a los elementos industriales o contra la red de producción, sino que irá dirigido a las redes perimetrales de control de datos adquiridos por y para los elementos de nivel 0 de una red de TO, así como hacia las de control SCADA.
- Con la aparición del 5G como nueva tecnología de comunicaciones en redes móviles, se crearán nuevas oportunidades para el diseño de nuevas amenazas, comprometiendo así los dispositivos de control con esta tecnología habilitada. Existen dispositivos remotos en la industria los cuales necesitan estar enviando datos a sus respectivos centros de control, desde ubicaciones completamente aisladas en donde sólo existe cobertura 4G y 5G.
- Coexiste una táctica bastante novedosa para el desarrollo y ejecución de nuevas taxonomías en ciberataques. Esta son las consistentes en ciberataques en "enjambre" (*Swarm-Bots, SB, por sus siglas en inglés)*. Los dispositivos, de los cuales van a hacer uso los atacantes, se encuentran agrupados por especialidades en las acciones a llevar a cabo, son dirigidos a las redes o dispositivos como un sistema constituido y comparten inteligencia en tiempo real para así perfeccionar su ataque según se produce.
- Una de las situaciones más peligrosas que se prevé aflore con fuerza será el ataque dirigido a las áreas de influencia y perimetrales de las redes de

las TO mediante una variante del *ransomware EKANS*[54], especializado en ataque de entornos industriales que cifre comunicaciones y datos correspondientes a los niveles 2 y 3 de los entornos de operación. En infraestructuras críticas serán generados cantidades ingentes de datos, existirán más dispositivos conectados (directamente o en remoto, incluso a través de la "nube") y, en consecuencia, existirán más vidas humanas dependientes de estas situaciones. Por consiguiente, éstas se verán en un serio compromiso cuando dependan de elementos como sensores y dispositivos de campo en el área de influencia perimetral de las TO y se conviertan en objetivos de los ciber-delincuentes[55].

Sobre la manera de adaptación por parte de la industria hacia la forma de tomar el pulso del estado de sus instalaciones, se prevé una potenciación de la búsqueda y rastreo activo. El hecho imparable de que los ciberataques seguirán mejorando en calidad, sofisticación y número, año tras año, provocará que las organizaciones actúen y combatan estas nuevas amenazas con tácticas diferentes.

La monitorización pasiva del tráfico en redes industriales ya no será suficiente, ya que en el futuro será necesario buscar amenazas de una forma más activa. Este hecho origina cierto debate ya que al tratarse de análisis activos, puede que estos tengan cierta repercusión en el proceso, como se ha explicado en la sección anterior.

[54] Es una variante descubierta en diciembre de 2019 que está especializada en el ataque a entornos industriales y otros ambientes en los que estén desplegados SCI. Provoca la paralización de las plantas productivas de dichos entornos industriales que son infectados, u otros entornos que tengan desplegados para su funcionamiento dispositivos pertenecientes a este ámbito industrial.

[55] Los ciber-delincuentes son aquellos ataques que se sirven de medios digitales para cometer delitos tradicionales, como la estafa, amenazas, acoso, extorsión, fraude, venta de productos falsos, entre otros.

Para ello será necesario el uso de fuentes externas de datos de seguridad o la integración de elementos como los sistemas de información y gestión de eventos (SIEM por sus siglas en inglés) que recogen eventos y registros de diferentes dispositivos y los centralizan, entre otras opciones en centro de operaciones de seguridad (Security Operation Center, SOC, por sus siglas en inglés) para su análisis.

Otros elementos que se deben tener en cuenta son los cortafuegos de nueva generación. Éstos ayudarán a solventar problemas de gran complejidad a nivel de red. Además, mejorarán la comunicación e intercambio de información dentro de la comunidad de las TO, que será clave a la hora de poder identificar rápidamente las amenazas.

Se deberán implantar sistemas que estén monitorizando continuamente las redes de control. A pesar del incremento de la seguridad y del uso de protocolos cifrados, la monitorización será uno de los aspectos más relevantes dentro de la ciberseguridad industrial.

Esta monitorización permitirá identificar nuevos ciberataques y activos que se incorporen a las redes monitorizadas.

Este tipo de herramientas tendrán que evolucionar para poder tratar el tráfico cifrado, con los inconvenientes que eso pueda generar dada la poca permisibilidad referente a las latencias en las TO.

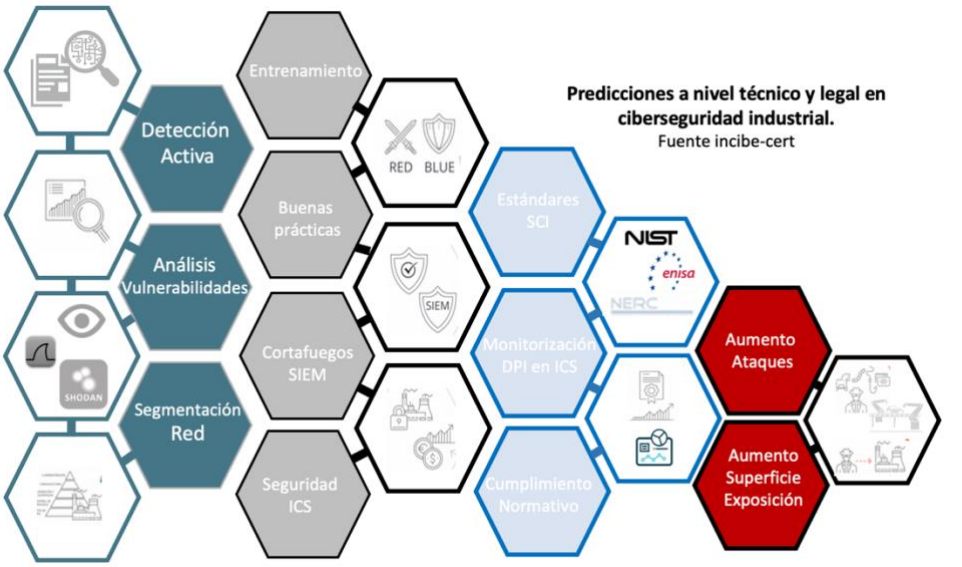


Figura 20: Representación gráfica de una posible predicción a nivel técnico y legal en ciberseguridad. (modificada de la fuente original INCIBE-CERT).

La Figura 20, viene a plasmar gráficamente los aspectos y relaciones existentes a nivel técnico y a su vez, legal, según las predicciones que el Instituto Nacional de Ciberseguridad ha realizado durante el pasado año 2020.

Muchas organizaciones siguen el modelo de Purdue cuando ejecutan una implantación de red industrial, de forma que cada sector industrial posee diferentes tipos de infraestructuras a nivel de red y pueden diferir en varios aspectos. Entre las modificaciones que podrán notarse se encuentra una posible modificación del propio modelo Purdue, el cual generaría variaciones no definidas claramente y por consiguiente carente de estandarización (posible regreso del concepto de seguridad por oscuridad).

Otro de los posibles puntos de apertura hacia la inseguridad cibernética recaerá sobre el aumento de la superficie de exposición. La

creciente cantidad de sistemas de automatización, la variedad de herramientas, el número de organizaciones y personas con acceso directo o remoto a estos sistemas, así como la aparición de canales de comunicación para la supervisión y el control remoto entre dispositivos que antes eran independientes, acrecientan las oportunidades de los ciber-delincuentes para planificar y ejecutar sus ataques. A la vez, el interés de los potenciales atacantes por los entornos industriales está aumentando considerablemente. Esto es debido a que, por contra partida, los ataques hacia las víctimas tradicionales están perdiendo interés por involucrar una disminución de la rentabilidad y un aumento del riesgo en ser detectados.

El aspecto fundamental, y que ya se está posicionando como clave para una defensa activa de los entornos industriales, es la planificación y ejecución de ejercicios de carácter equipo rojo y equipo azul (Red Team us Blue Team, RT-BT, por sus siglas en inglés). Este tipo de ejercicios, en los que se emularán o simularán ciberataques, permitirán entrenar tanto a equipos defensivos como de ataque. A nivel defensivo proporcionarán un conocimiento sobre las pautas a seguir frente a un incidente; y por la parte ofensiva permitirá tener un mayor conocimiento de los entornos industriales [URL- 43, 2021].

No solo el marco técnico y operacional es susceptible de sufrir cambios con el paso del tiempo, de igual forma en el ámbito legal habrá nuevos enfoques a la hora de seguir una guía de buenas prácticas con la que cumplir las exigencias de los diferentes estándares o normativas que involucren a las diferentes industrias.

Las predicciones más significativas a nivel legal para el futuro son las siguientes:

- **Aparecerán nuevos estándares para la seguridad de SCI.** Será importante ver la evolución que conllevarán las nuevas normativas y estándares

específicos para los sistemas de control industrial. En este ámbito es muy posible que aparezcan nuevos modelos específicos a nivel sectorial y de comunicaciones. Por otro lado, aumentarán los estándares que permitan obtener certificaciones de producto como la IEC 62443 4-2.

- **Cambios en el cumplimiento legal.** Estas variaciones en los cumplimientos legales afines a la ciberseguridad industrial suelen encontrarse en los estándares de la Comisión Internacional de Electrotécnica (International Electrotechnical Commission, IEC, por sus siglas en inglés) y que, a su vez, están propiciados por los cambios en la tecnología.

El período actual de desarrollo para estos estándares corresponde a cinco años, lo cual es extremadamente lento, tornándose complicado obtener una mejora a corto plazo.

El sistema actual asegura que el estándar sea un documento de consenso que ha sido considerado por muchas personas de diferentes orígenes. Además, será importante que esta evolución y cumplimiento de las normativas se tengan en cuenta tanto a nivel nacional como europeo.

3.3. Marco legislativo y normativo

Como ya quedó reflejado en el Capítulo I, esta investigación se ha llevado a cabo en el área de la ciberseguridad en entornos industriales y, más concretamente, trata de proporcionar un valor diferenciador en el campo de los servicios esenciales [Anna S., 2016], [Wang S., 2016]. Estos servicios esenciales son prestados por lo que actualmente se denominan infraestructuras estratégicas y/o críticas [European Commision., 2005], [Council D., 2008], [Directive (EU), 2016]. Estas infraestructuras han adoptado una posición relevante en la gestión de riesgos y crisis de cualquier país. Por lo tanto, la ciberseguridad involucrada en los SCI es clave para el

funcionamiento normal del orden social de un país. Aunque las definiciones de infraestructura crítica varían de un estado a otro, prácticamente todos los países identifican los tipos de infraestructura en función de los servicios que prestan [Directive, 2008], [Directive, 2016]. Concretamente, se trata de las centrales y redes eléctricas, las tecnologías de la comunicación y la información, las finanzas, la salud, los alimentos, el agua, el transporte, la producción, el almacenamiento y el transporte de productos peligrosos. En España se promulgó la Ley de Protección de Infraestructuras Críticas (LPIC) [Ley PIC, 2011] y todos sus puntos han sido implementados en el Reglamento de Protección de Infraestructuras Críticas (RPIC) [Real Decreto, 2011]. El origen de esta regulación nacional emana de la Directiva Europea, Directiva 2008/114/CE[56] por la que se designan e identifican un total de 41 infraestructuras críticas europeas, constatando en paralelo la necesidad de mejorar su protección evaluando su situación actual como punto de partida [Critical Infrastructure, 2016].

En España se han definido doce sectores estratégicos directamente implicados en la LPIC y se han dividido en subsectores: administración, espacio, industria nuclear, industria química, instalaciones de investigación, agua, energía, salud, tecnologías de la información y la comunicación, transporte, alimentación y sistema financiero y fiscal.

A su vez, la Estrategia de Seguridad Nacional (ESN) de 2011 [Real Decreto 385, 2013], [Real Decreto 3, 2010] considera las ciber-amenazas y los ciberataques como elementos principales que proporcionan un alto índice de riesgos para la seguridad nacional. Una ESN renovada y que ampliaba los conceptos y áreas de aplicación de su predecesora fue aprobada

[56] Directiva 2008/114/CE del Consejo de Europa de 8 de diciembre de 2008 sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección; https://www.boe.es/doue/2008/345/L00075-00082.pdf

en el año 2013. Este documento es considerado primordial para la ciberseguridad de España. Esta estrategia mejorada ayudó a definir nuevos escenarios estratégicos y a involucrar más activamente a la sociedad civil en la seguridad nacional. En su cuarto capítulo, dedicado a las líneas de acción clave, la ESN identifica la ciberseguridad como una de las doce áreas de trabajo prioritarias. El desafío de la seguridad cibernética es equiparable con las amenazas tradicionales, como el terrorismo. Como resultado de las preocupaciones expresadas en la ESN del 2013, a través de la Estrategia Nacional de Ciberseguridad (ENCS) fue elaborado un marco de políticas y una estructura ejecutiva para impulsar la ciberseguridad como una de las principales prioridades a adoptar en la seguridad nacional. A modo de resumen gráfico, la Figura 21 detalla las diferentes apariciones de las estrategias españolas ordenadas cronológicamente.

La definición del rumbo a seguir referente a la ciberseguridad en los entornos industriales se encuentra supeditada a un mantenimiento en el tiempo de la disponibilidad de sus ecosistemas de producción, y de la información necesaria disponible en tiempo real mediante la interconexión de todos los elementos que participan en la cadena de valor, como fruto de la CTIO.

Figura 21: Imagen resumen de las estrategias establecidas por el Gobierno de España 2011-2019.

Si se quieren cumplir con los objetivos buscados, este flujo de información se tiene que mantener de manera continua y uniforme a lo largo del tiempo, a la vez que seguro, y esto debe hacerse necesariamente bajo el marco de métodos que indiquen las directrices de su normalización y regulación (ver Figura 21).

Ante esta situación tan sumamente novedosa se ponen en juego valores tan importantes como la seguridad y el bienestar de los Estados y sus ciudadanos.

Desde la última década, el sector industrial se encuentra en el proceso de plena demanda de normativa concerniente a la ciberseguridad, para así lograr y afianzar un alto grado de seguridad y protección para sus instalaciones. A su vez y como consecuencia directa de la problemática asociada por su catalogación de estas industrias como infraestructuras críticas estatales, afloran normativas reguladoras, consecuencia directa del decidido impulso que se está otorgando a la protección de servicios esenciales en los que se encuentran involucrados sistemas de TI y TO.

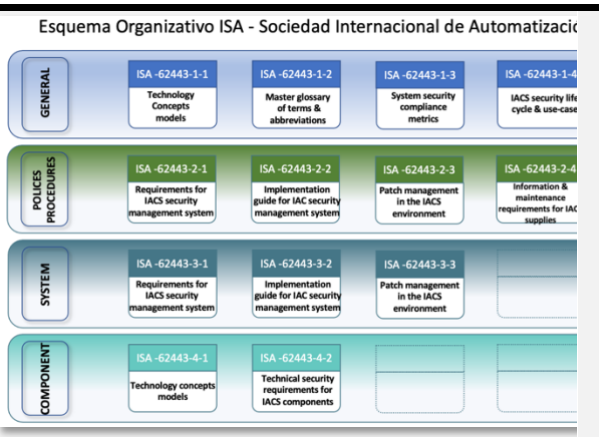
Fruto de ello han surgido un gran conjunto de normas y guías de seguridad de las que, tras haber realizado un proceso exhaustivo de investigación al respecto [URL- 44-45-46-47-48-49, 2021] se recogen las más

relevantes en la Tabla 13, y que afectan a las TI y las TO, indicando las características más significativas de cada una de ellas.

Norma estándar	Breve descripción	URL referencia
	Desarrollo - Nacional -	
• **Real Decreto 421/2004**	Por el que se regula el Centro Criptológico Nacional (CCN-CERT).	URL- 50
• **Consejo Ministros 11/2007**	Acuerdo de Consejo Ministros, Protección Infraestructuras Críticas.	URL- 51
• **Real Decreto 3/2010**	Por el que se regula el Esquema Nacional de Seguridad (Administración Electrónica).	URL- 52
• **Ley 8/2011**	Por la que se establecen medidas para la Protección de Infraestructuras Críticas.	URL- 53
• **Real Decreto 704/2011**	Por el que se aprueba el Reglamento de Protección de las Infraestructuras Críticas.	URL- 54
• **Estrategia de Seguridad Nacional 2011**	Por la que se establecen líneas de actuación básicas ante amenazas y riesgos transversales a nivel nacional.	URL- 55
• **Estrategia de Seguridad Nacional 2013**	En su cuarto capítulo, dedicado a las líneas de acción clave, la ESN identifica la ciberseguridad como una de las doce áreas de trabajo prioritarias.	URL- 56
• **Estrategia de Seguridad Nacional 2017**	Establece que la política de seguridad nacional es una política pública para responder a las necesidades de la seguridad nacional.	URL- 57
• **Real Decreto-Ley 12/2018**	Seguridad de las redes y sistemas de la información.	URL- 58
• **Estrategia Nacional de Ciberseguridad 2019**	Se pone de manifiesto la importancia del ciberespacio como espacio común global, así como las ciberamenzas y desafíos a afrontar como nación.	URL- 59
• **Estrategia Nacional Inteligencia Artificial 2020**	Con la que se pretende impulsar la investigación científica, el desarrollo tecnológico y la innovación en IA.	URL- 60
• **Real Decreto 734/2020**	Por el que se desarrolla la estructura básica del Ministerio del Interior, cambios organizativos en CNPIC	URL- 61
• **Real Decreto 43/2021**	Por el que se desarrolla el Real Decreto-Ley 12/2018, seguridad en redes y sistemas de la información	URL- 62

• **Anteproyecto de Ley sobre los requisitos para garantizar la seguridad de las redes y servicios 5G- 2021**	Borrador del anteproyecto de ley sobre los requisitos para garantizar la seguridad de las redes y servicios 5G.	URL- 63
	- Europeo -	
• **Directiva europea NIS 2016**	Relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.	URL- 64
• **Reglamento europeo Directiva NIS 2020**	Establece los procedimientos que deberán tener en cuenta los operadores y proveedores para gestionar y resolver los incidentes de seguridad. Asimismo, el nuevo reglamento NIS marca las directrices sobre cómo han de notificarse los incidentes que afecten a las redes y sistemas de información utilizados.	URL- 65
• **The EU's Cybersecurity Strategy for the Digital Decade 2020**	Nueva estrategia de ciberseguridad de la UE y nuevas normas para hacer más resistentes las entidades críticas físicas y digitales.	URL- 66
	- Global -	
• **National Cybersecurity Protection Act of 2014**	Ley para establecer una asociación voluntaria y permanente entre el sector público y el privado con el fin de mejorar la ciberseguridad y reforzar la investigación y el desarrollo de la ciberseguridad.	URL- 67
• **The National Security Strategy: Authorities, Changes, Issues for Congress 2015**	El 6 de febrero de 2015, la Administración Norte americana publicó una nueva Estrategia de Seguridad Nacional (NSS). Este documento afirma que su objetivo es "establecer los principios y las prioridades para guiar el uso del poder y la influencia de Estados Unidos en el mundo".	URL- 68
• **NIST Small Business Cybersecurity Act 2017**	Este proyecto de ley modifica la Ley del Instituto Nacional de Normas y Tecnología para exigir al Instituto Nacional de Normas y Tecnología (NIST) que tenga en cuenta a las pequeñas empresas cuando facilite y apoye el desarrollo de directrices y procedimientos voluntarios, basados en el consenso y dirigidos por la industria, para reducir de forma rentable los riesgos cibernéticos para las infraestructuras críticas.	URL- 69

• **Cybersecurity National Action Plan 2018**	Plan estratégico por el que se desarrolla la metodología para la mejora de la gestión de los riesgos de ciberseguridad a nivel nacional, aumentando la seguridad y la resistencia de las redes gubernamentales y las infraestructuras críticas; disminuyendo la actividad cibernética ilícita; mejorando las respuestas a los incidentes cibernéticos; y fomentando un ecosistema cibernético más seguro y fiable.	URL- 70
• **Us Department of Homeland Security Cybersecurity Strategy 2018**	Esta estrategia proporciona al Departamento un marco para ejecutar nuestras responsabilidades en materia de ciberseguridad durante los próximos cinco años para seguir el ritmo de la evolución del panorama de los riesgos cibernéticos mediante la reducción de las vulnerabilidades y obtención de mejoras en resiliencia.	URL-71
• **National Strategy to Secure 5g of The United States of America 2020**	Esta estrategia proporciona al Departamento un marco para el despliegue de las tecnologías 5G, de manera segura y en beneficio de una mejora en ciberseguridad y ciber-resiliencia.	URL- 72
• **National Cyberspace Security Strategy 2016**	Estrategia nacional para la salvaguarda de la ciberseguridad ante los nuevos riesgos, aplicando medidas importantes para avanzar en la disposición estratégica de construir integralmente una sociedad moderadamente próspera y ciber-segura.	URL- 73
• **National Cyber Security Strategy of Afghanistan (NCSA) 2014**	Su objetivo es obtener un ciber ecosistema seguro y resiliente, generando un marco de trabajo para la seguridad de la información y las garantías de las políticas de seguridad.	URL- 74
• **National Security Strategy 2009-2020**	Las principales orientaciones de la política de seguridad nacional de la Federación Rusa son las llamadas prioridades nacionales estratégicas en forma de importantes transformaciones sociales, políticas y económicas para el desarrollo estable del país y la preservación de la integridad territorial y la soberanía del Estado.	URL- 75
Estándares		
• **IEC 61850**	La Comisión Electrotécnica Internacional (CEI), también conocida por su sigla en inglés IEC (International Electrotechnical Commission), es una organización de normalización en los campos eléctrico, electrónico y tecnologías relacionadas. Especialmente la norma 61850 ha sido definida y creada para la automatización de subestaciones eléctricas.	URL- 76

• **IEC 62443**	 La norma IEC 62443, elaborada por el grupo TC65 de la IEC, surge como evolución de la norma ISA 99, con la intención completarla y ampliar sus capacidades de actuación. Los documentos se dividen en 5 informes técnicos, 1 especificación técnica y 7 guías, agrupadas en cuatro bloques según su contenido: general, políticas y procedimientos, sistema y componentes.	URL- 77
• **IEC 62351**	El ámbito de actuación de la norma IEC 62351 es la seguridad en las operaciones de control del sector energético. El objetivo principal es acometer el desarrollo de estándares de seguridad para los protocolos de comunicaciones definidos por el grupo IEC TC 57, específicamente IEC 60870-5 (IEC101, IEC104, etc.), IEC 60870-6 (ICCP), IEC 61850 (MMS, GOOSE), IEC 61970 y IEC 61968.	URL- 78
• **ISA99**	La norma ISA99 engloba un conjunto de guías e informes técnicos, de los que están publicadas ANSI/ISA-99.01.01-2007 y ANSI/ISA-99.02.01-2009 y un informe técnico SI/ISA-TR99.01.02-2007.	URL- 79
• **NIST**	Instituto Nacional de Estándares y Tecnología (Departamento de Comercio de EEUU). • **SP 800-82:** Su propósito es proporcionar una guía para la seguridad de los sistemas de control, incluyendo sistemas SCADA (Supervisory Control And Data Acquisition), DCS (Distributed Control System) y otros sistemas que trabajan en los sistemas de control. • **SP 800-53:** El propósito de la publicación es proporcionar una guía de controles de seguridad para los sistemas de información. Se aplica a todos los componentes de un sistema de información que procesa, almacena o transmite información.	URL- 80

• **NRC-RG**	La comisión de regulación nuclear de los Estados Unidos (NRC) publicó esta guía para establecer los controles para el cumplimiento de las regulaciones de la comisión respecto a la protección de los ordenadores, las comunicaciones y las redes frente a ciberataques. • **La guía RG 5.71** (Regulatory Guide 5.71, [URL- 81-a, 2010]) describe una estrategia de defensa consistente en una arquitectura defensiva y un conjunto de controles.	URL- 81
• **NERC CIP**	El NERC es el organismo regulador de la energía de los Estados Unidos. Para poder valorar la seguridad de las instalaciones y del sector en general creó una serie de guías con controles de obligado cumplimiento. Originalmente crearon 9 guías, de las que todas menos la primera, están relacionadas con la ciberseguridad. Posteriormente ampliaron el número total a 11. Actualmente está en vigor la versión 3 y en desarrollo la versión 5 (excepto para CIP-010 y CIP-011 que es la versión 1).	URL- 82
• **IEEE**	• **IEEE 1686-2007:** El estándar IEEE 1686-2007 define las funciones y características que deben ser proporcionadas por los IED (Intelligent Electronic Device) para acomodarse a los programas CIP (Critical Infrastructures Protection). • **IEEE 1711-2010:** Define un protocolo serie de seguridad para dos tipos de módulos criptográficos: el módulo criptográfico SCADA (SCM) para proteger el canal serie SCADA; y el módulo criptográfico de mantenimiento (MCM) para proteger el canal de manteamiento, habitualmente implementado sobre modem.	URL- 83
• **API 1164**	Esta norma sobre la seguridad de SCADA proporciona orientación a los operadores de sistemas de oleoductos y gasoductos para gestionar la integridad y seguridad del sistema SCADA. El uso de este documento no se limita a los oleoductos regulados por el Título 49. CFR 195.1, debe considerarse como una lista de las mejores prácticas que deben emplearse al revisar y desarrollar normas para un sistema SCADA.	URL- 84

Tabla 13: Tabla resumen de normas y estándares que afectan a las TI y las TO.

3.3.1. Laboratorios de pruebas

Una vez analizadas las problemáticas asociadas por la irrupción de las nuevas amenazas en las que se están viendo involucrados los sistemas de control industrial y, en paralelo, lo complicado que resulta poder realizar testeos de seguridad en estos sistemas en entornos de infraestructuras críticas, ¿cuál sería el siguiente paso a llevar a cabo?

En el momento en que se define un SGCI por parte de una organización, en la 3ª etapa, queda detallada la promoción de una cultura de ciberseguridad entre los componentes de la entidad (ver Sección 3.2.4.1). Esta actividad involucra al personal y a las tecnologías. Para comprender este paradigma se puede observar la Figura 22, la cual representa el concepto de defensa en profundidad que, como tal, viene a definir un modelo basado en la creación y definición de una serie de medidas para la protección máxima de los sistemas de control industrial, concretamente para proteger su disponibilidad. Estas medidas han sido concretadas como objetivos a proteger y definir a través de SICERCAI, sistema que involucra en sus evaluaciones aspectos TI, TO y del ámbito de la gestión, entendiendo ésta como aquellas actividades necesarias para la culminación de las diferentes actividades para la utilización de recursos (materiales y humanos).

Como se ha señalado, y dada la relevancia de los procesos llevados a cabo en la industria, y más concretamente los clasificados como críticos, no es posible exponer esta infraestructura a un proceso experimental directo.

Como ayuda a la transición de este proceso surge el concepto de laboratorios físicos o virtuales de accesos remotos o locales.

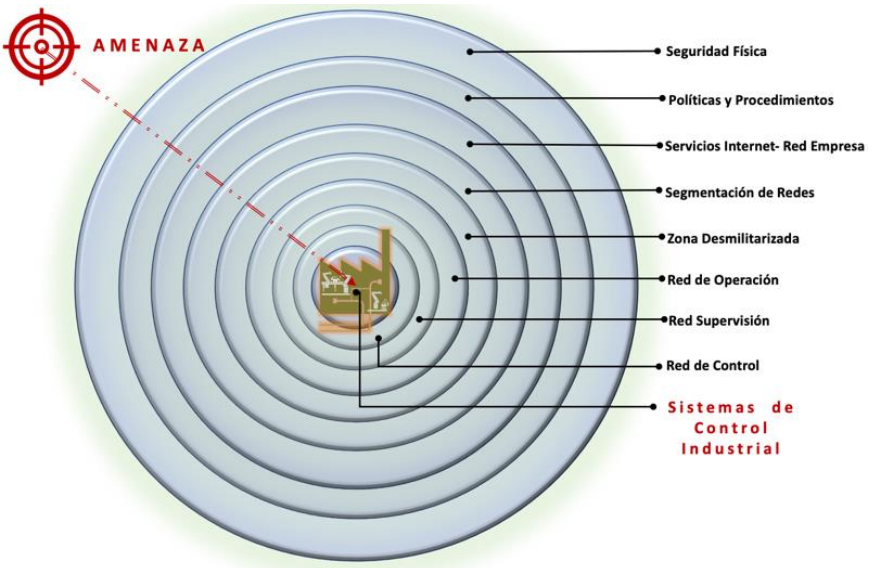


Figura 22: Representación ilustrativa del concepto de defensa en profundidad.

	Real	Virtual
Local	Laboratorios físicos, presenciales y ubicados en plantas reales.	Laboratorios presenciales con plantas simuladas a través sistemas informáticos.
Remoto	Procesos de tele-operación en plantas reales.	Laboratorios remotos con plantas y procesos simulados a través de sistemas informáticos.

Tabla 14: Principales clasificaciones de laboratorios de pruebas.

La Tabla 14, aclara las propiedades de cada uno de ellos [Sánchez M., 2015].

Referente a los laboratorios físicos de pruebas, existe una extensa literatura en éste área [Yamin M., 2020], [Noorizadeh M., 2021], [Ani J., 2020], la cual revela el refuerzo que exige la mejora, y sobre todo la capacidad de adelantarse a la problemática sufrida por los SCI en la seguridad de los procesos, todo ello como resultado del aumento del número de los ciber-incidentes soportados. Estos laboratorios de pruebas combinan varios modelos de sistemas enfocados hacia los componentes industriales para así

crear un modelo con una funcionalidad física de los procesos, creados, gestionados y administrados en un entorno de producción funcional entre redes de TI y TO.

Esta arquitectura específica se encuentra lastrada por su carácter estático en el modelo a ejecutar-evaluar. Dado el alto coste de los componentes industriales es comprensible esta limitación, ya que no todas las instituciones-organizaciones se pueden permitir desplegar en un solo y único entorno de pruebas la totalidad de la casuística que se puede llegar a producir o demandar.

Desde el ecosistema universitario se está viendo potenciada la capacidad de aporte de conocimiento en la mejora de la resiliencia de los SCI como resultado de las investigaciones que se llevan a cabo. En paralelo a estas iniciativas se encuentran otras propiciadas por entidades privadas relacionadas con el control de automatismos industriales. En España a finales del año 2015 se presentó, por iniciativa del Instituto Nacional de Ciberseguridad, [57], la Red Nacional de Laboratorios Industriales (RNLI) [URL-85, 2021]. Esta red está basada en la disponibilidad de un conjunto entornos de pruebas de diferentes naturalezas y especializados en los sectores estratégicos para la obtención de conocimiento que posibilite la mejora en capacidades de seguridad de infraestructuras industriales de España.

A través de esta RNLI se proporciona un punto de unión entre la oferta y la demanda de la seguridad en los entornos industriales a nivel nacional, se pone a disposición de toda la comunidad relacionada con la seguridad

[57] INCIBE-CERT es el centro de respuesta a incidentes de seguridad de referencia para los ciudadanos y entidades de derecho privado en España operado por el Instituto Nacional de Ciberseguridad (INCIBE), dependiente del Ministerio de Asuntos Económicos y Transformación Digital, a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial.

industrial información sobre infraestructuras nacionales y se promueve a su vez la colaboración y cooperación entre los actores involucrados en la seguridad de estos entornos (colaboradores públicos y privados). Además, se fomenta el intercambio de conocimiento dentro de la comunidad, mejorando así el nivel de seguridad de las infraestructuras dotadas de sistemas de control industrial.

En la actualidad la red cuenta con veinticinco laboratorios propiedad de diferentes organizaciones. SICERCAI, junto con una maqueta industrial de procesos de simulación de elementos químicos, la cual se encuentra ubicada en el laboratorio del Departamento de Informática y Automática de la Universidad Nacional de Educación a Distancia (UNED) son candidatos a ser incluidos en esta RNLI.

A nivel europeo existe la propuesta para la creación de un banco de pruebas de sistemas SCADA para proporcionar instalaciones de ensayo real para investigadores académicos y otras partes interesadas, así como para los propios fabricantes de estos sistemas de supervisión, control y adquisición de datos [Christiansson H., 2008].

Viniendo a ampliar la red de laboratorios industriales existentes, el Instituto Tecnológico de la Columbia Británica (British Columbia Institute of Technology, BCIT, por sus siglas en inglés) alberga un banco de pruebas de sistemas SCADA conocido como el "*Laboratorio de Procesos de Instrumentación Industrial*" (LPII) [URL- 86, 2021]. El LPII del BCIT incluye una columna de destilación, un evaporador, un digestor de pulpa por lotes, un proceso de reacción de mezcla química y una caldera de energía, siendo capaz de simular procesos de la industria química. Además, incluye una variedad de equipos SCADA que incluyen sistemas de control distribuido de diferentes modelos y fabricantes (Emerson, DeltaV y Provox), así como una amplia gama de controladores.

Los investigadores académicos han utilizado diversas estrategias para apoyar las pruebas de las soluciones de ciberseguridad de los sistemas de control industrial propuestos, y las soluciones de ciberseguridad de SCI designados, incluyendo instalaciones SCADA a pequeña escala reales y virtuales. Varias de estas iniciativas se encuentran desplegadas en los laboratorios miembros de la RNLI.

Múltiples grupos de investigación han propuesto sistemas basados en la simulación para diseñar sistemas de control, sus redes de comunicación y los ataques de ciberseguridad contra un SACI. En [Jim M., 2010] se analiza el uso de la simulación en el ámbito de los sistemas de control industrial para el diseño y el modelado de técnicas, procesos, formación de los operadores y la definición de metodologías de respuestas ante los incidentes.

La mayoría de los bancos de pruebas de seguridad de un sistema SCADA incluyen un simulador de procesos, virtualizadores de red y un mecanismo para iniciar un ciberataque al sistema.

En [Charles M., 2006] se acomete un enfoque basado en la simulación para modelar el sistema de energía eléctrica. Este es realizado mediante la unión del simulador Power-World (software especializado), de clientes de red virtuales, controlando y simulado las mediciones obtenidas del sistema eléctrico replicado, así como el entorno de simulación de red inmersiva[58] en tiempo real, para recrear el tráfico de red y posibles ataques que afectarían a la ciberseguridad.

En [Bello R., 2020] se pretende identificar las principales metodologías de evaluación del riesgo en seguridad aplicadas a sistemas SCADA enfocado a infraestructura críticas, en concreto a compañías eléctricas. Toman como

[58] La tecnología inmersiva se refiere al tipo de tecnología que intenta emular un mundo físico a través de un mundo digital o simulado, creando así un sentido de inmersión.

prioritarios aquellos documentos en los cuales las metodologías son experimentales, preferiblemente con resultados aceptables, y aquellas con planteamientos adecuados en los que se espera la implementación y pruebas con buenos resultados.

En [Lu K., 2021] se presenta para su utilización un método de detección de redes de creencia profunda basado en la optimización extrema de la población (PEO-DBN, Population Extremal Optimization-Deep-Belief-Network, por sus siglas en inglés) para detectar los ciberataques de los sistemas de identificación y codificación del sector industrial (Industry Standard Coding Identification, ISCI, por sus siglas en inglés) basados en SCADA. En el método PEO-DBN se emplea el algoritmo PEO para determinar los parámetros ajustables de la DBN, incluyendo el número de unidades ocultas, el tamaño del mini-batch y la tasa de aprendizaje [URL- 87, 2019], ya que no existe un conocimiento claro y profundo para establecer esos parámetros.

A nivel extrafronterizo europeo es destacable la función desempeñada desde el Laboratorio Nacional de Idaho (Idaho National Labs, INL, por sus siglas en inglés). El INL forma parte del complejo de laboratorios nacionales del Departamento de Energía de Estados Unidos. Se encuentra incluido en un programa de banco de pruebas a gran escala cuyo objetivo es contribuir a la evaluación de la ciberseguridad de los sistemas de control, la mejora de estándares y normas, la divulgación y la formación. En la Sección 3.2.7.2 se detalló uno de los proyectos más importantes llevados a cabo en el INL en materia de exposición a un ciberataque a una infraestructura física: el Proyecto AURORA [URL- 00, 2021].

El laboratorio de pruebas SCADA del INL incluye una red eléctrica a escala completa. La red eléctrica del INL incluye un bucle de transmisión de 128 kV de 61 millas, líneas de distribución de 13,8 kV, y 7 subestaciones con

más de 3.000 puntos de supervisión y control en el sistema. Además, posee el banco de pruebas SCADA. A su vez el INL es el principal centro de investigación y desarrollo de energía nuclear del país.

3.3.1.1. Laboratorios virtuales y remotos

Los diferentes estamentos y organizaciones detalladas con anterioridad, corresponden con las principales iniciativas existentes que en la actualidad y a nivel global existen y se encuentran desplegadas como laboratorios de pruebas para la mejora de la ciberseguridad de los SACI.

En paralelo han emergido varias problemáticas asociadas a estas iniciativas, como son el espacio necesario para su despliegue, la especialización, la pasividad ante cambios y variaciones, la dedicación de entornos, y, sobre todo, su elevado coste. Para compensar estos inconvenientes, la tecnología ofrece posibilidades mediante el desarrollo de nuevos conceptos en entornos de pruebas y evaluación, surgen los laboratorios remotos y virtuales.

Como se especifica en el estudio denominado *"Laboratorios virtuales y remotos para la práctica a distancia de la automática "* [Dormido S., 2013], se puede definir que el concepto de laboratorio virtual y remoto viene a englobar y apoyar una solución para un conjunto de colectivos que exigen disponer de sistemas de enseñanza y evaluación con un alto carácter de flexibilidad, accesibilidad y de naturaleza adaptativa.

Durante la presente Tesis se ha señalado en varias ocasiones que, dada la relevancia de los procesos llevados a cabo en la industria y más concretamente los clasificados como pertenecientes a IC, no es posible exponer estos sistemas a técnicas experimentales de modo directo. Por ese motivo, como ayuda a este proceso de transición emergente entre la experimentación real y la simulación, los conceptos de laboratorios virtuales

y remotos manan desde el ámbito de la investigación universitaria para ayudar en esta tarea.

Actualmente, la idea de la educación a distancia está firme y globalmente establecida en este campo. La puesta en escena de los avances tecnológicos, con la virtualización como componente principal, ha ayudado a esta consolidación [Bencomo S., 2004], [Sánchez J., 2002], [Zhang M., 2019].

Existe mucha literatura científica sobre el diseño y desarrollo de laboratorios remotos en diferentes áreas de investigación y enseñanza [Chacón J., 2015]. Los laboratorios remotos y virtuales son sistemas experimentales basados en una arquitectura de comunicación en la que el usuario y los dispositivos a controlar (simulados o reales) están separados geográficamente, siendo las TIC las encargadas de permitir a esos usuarios el acceso al equipo experimental [Cerezo F., 2015], [Del Canto J, 2015], [De la Torre L.,2016], [Sáenz J., 2019]. Estos espacios virtuales permiten a los usuarios realizar prácticas en tiempo real, visualizando las acciones ejecutadas mediante circuitos de televisión cerrados y cámaras web con direccionamiento IP. Estas arquitecturas soportan la incorporación de SICERCAI, utilizando como punto de partida el acceso a la célula de automatización industrial creada a través de localizaciones distribuidas espacialmente.

El objetivo corresponde directamente a la resolución de los tres aspectos fundamentales promulgados por la estrategia nacional de ciberseguridad, publicada en 2017 por el gobierno de España [URL- 88, 2017]: la enseñanza, el aprendizaje y la conmutación.

Debido a pandemia sufrida durante la realización de este trabajo de investigación, los procesos de enseñanza y aprendizaje se han puesto a prueba respondiendo de manera eficaz a los objetivos planteados. En el

estudio [Herrero D., 2021], se demuestran los grandes resultados obtenidos por la puesta en práctica de este tipo de enseñanza, forzada por la necesidad de confinamiento de la sociedad y pandemia sanitaria sufrida durante el año 2020.

Estos estudios fueron desarrollados en el primer cuatrimestre correspondiente al año 2020 en el ámbito universitario de la ingeniería industrial, los cuales demostraron la eficiencia del uso de estos, condicionados a la disposición de capacidad de cómputo e interconexión.

A su vez en [Vargas J., 2021] se presentan unos resultados relevantes sobre la aceptación y percepción por parte de los alumnos que utilizaron los laboratorios remotos de IOT, y que utilizaron esos entornos virtuales de acceso remoto durante el tiempo de estudio y evaluación (tiempos del COVID-19).

3.4. Honeypots

Para finalizar este capítulo, y tras haber realizado un análisis exhaustivo y habiendo obtenido una visión real de la situación de los actores involucrados en la evaluación, análisis y propuestas para la mejora de la ciberseguridad de un sistema de control industrial, es el momento de entrar en detalle del estudio de los denominados honeypots (HP)[59].

Entre las muchas soluciones de seguridad para la detección de redes o robots informáticos (botnets, por su definición en inglés) que se ejecutan de manera autónoma y automática para causar daños a infraestructuras de la TI como TO, se encuentran los HP. Por su naturaleza pueden estar creados y diseñados mediante software, hardware o ambos, simulando equipos y

[59] Se corresponden con sistemas reales o virtualizados, sistemas hardware o herramientas software, que simulan ser equipos vulnerables para poder exponerlos sin ningún riesgo y permitir el análisis de todos los ataques efectuados sobre ellos.

sistemas de automatización industrial. Mediante su uso se ha demostrado su eficacia en los primeros estudios llevados a cabo [Lee S., 2021].

En [Quiang F., 2021] se presenta un estudio que utilizando técnicas híbridas como son el uso de un modelo epidémico basado en un honeynet (HN)[60] en una red de un sistema de control industrial. Por otra parte la investigación llevada a cabo por Qiang Fu ha quedado formulado un modelo epidémico con inmunización y cuarentena en la red SCI, otorgando la capacidad de la exploración dinámica de la propagación del malware [Quiang F., 2020].

Además, los experimentos y los resultados numéricos obtenidos han demostrado que con el despliegue de uno de estos sistemas, altamente vulnerable, dentro de la red SCI, la infección producida mediante el malware se ha desarrollado en el HP. De igual manera, los experimentos de simulación proporcionan el comportamiento real de la propagación del malware en la red SCI, por lo que este despliegue mixto está abocado al éxito, aumentando así la capacidad de previsión de ciberataques a entornos TO.

3.4.1. Evolución de los Honeypots

Tras la introducción aclaratoria de conceptos, es necesario reseñar la evolución de estos sistemas y sus entidades desarrolladoras.

- **The Honeynet Project.** Uno de los principales proyectos a nivel mundial, promotores del uso de honeypots y honeynets, es *"The Honeynet Project"* [URL- 89,2021]. Fundado en 1999, ha contribuido a la lucha contra el malware y los ataques de hacking maliciosos durante más de dos décadas. Su principal misión es conocer las herramientas, tácticas y motivos de los ataques informáticos y de red con el fin de compartir las lecciones

[60] Las honeynet son un tipo especial de los honeypots, los cuales se caracterizan por su alta interacción sobre una red entera de sistemas.

aprendidas. En la Figura 23 se detalla un ejemplo arquitectónico de una HN.

- **Honeyd.** Es un software desarrollado por Niels Provos [URL- 90, 2021] consistente en la creación y ejecución de múltiples HP a través de entornos virtuales.

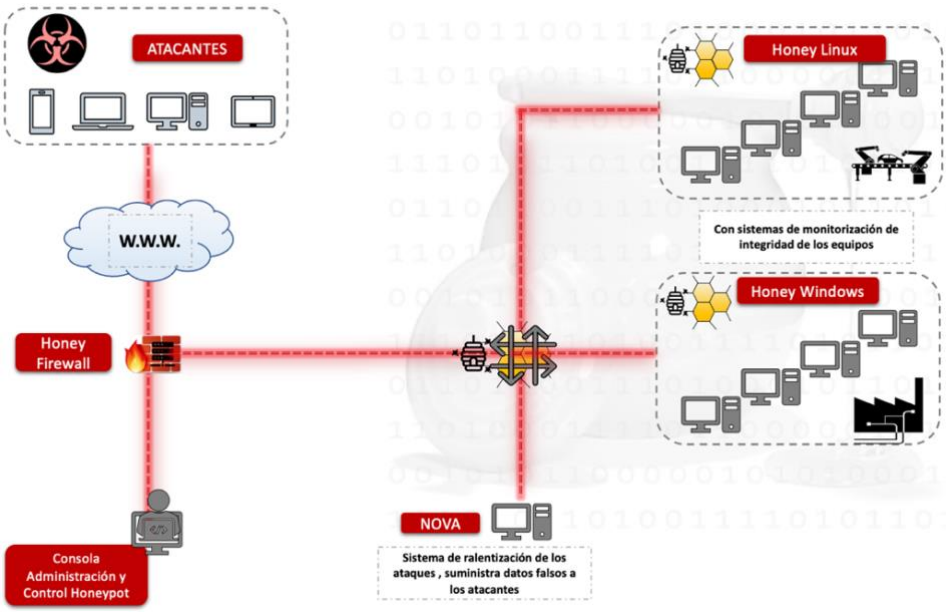


Figura 23: Detalle de una posible arquitectura de una Honey Net.

Su principal objetivo es conseguir generar una distracción de los atacantes retrasando y ralentizando las posibles acciones a llevar a cabo, todo ello orientado a la obtención de conocimiento de las diferentes taxonomías de los ataques.

- **Conpot & Gaspot.** Una de sus principales ventajas es la facilidad de su despliegue y modificación. En la actualidad el proyecto se encuentra integrado dentro de *"The Honeynet Project"*. Por defecto, el PLC que simula es un S7 200 de SIEMENS bajo protocolo MODBUS, SNMP y HTTP [URL- 91, 2021].
- **Honeynet SCADA (Digital Bond).** Su objetivo principal consiste en la construcción de un software para la simulación de una amplia gama de

dispositivos industriales. Su despliegue se apoya en el uso de Honeyd y, a través de un sistema operativo Linux, simular multitud de dispositivos y redes industriales [URL- 92, 2021].

Ya en nuestros días existen infinidad de organizaciones (públicas y privadas) las cuales están inmersas en diferentes proyectos para la mejora del aprendizaje de los ciberataques dirigidos contra sistemas de control y, más concretamente, los involucrados en operaciones críticas. En el repositorio de documentación habilitado para la presente Tesis se encuentra ubicado un archivo en formato PDF[61] denominado "Catálogo de empresas de ciberseguridad 2016" el cual corresponde a la documentación creada respecto a la información expuesta con anterioridad [URL-00, 2021].

3.4.2. Clasificación de honeypots

La clasificación de estos sistemas se puede realizar basándose en diferentes características funcionales, lo cual facilita su elección según las necesidades requeridas.

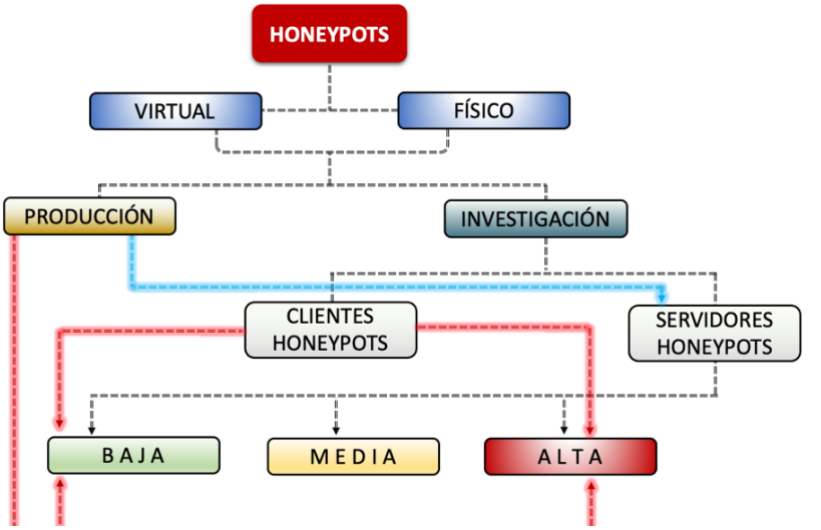


Figura 24: Catalogación de sistemas Honeypots (modificada de la fuente original: INCIBE-CERT).

[61] Portable Document Formar, PDF, por sus siglas en inglés, se corresponde con un formato de almacenamiento para documentos digitales, siendo de tipo compuesto (imagen vectorial, mapa de bits y texto).

Según el Instituto Nacional de Ciberseguridad (INCIBE-CERT) y como se esquematiza en la Figura 24, una posible clasificación de las honeypots puede ser la siguiente:

- ***Tipo de Equipamiento*.** El tipo de equipamiento hace referencia a las plataformas de despliegue, físicas o virtuales.
  - *Físico.* Como su propio nombre indica, corresponde a un sistema real conectado al exterior para poder ser atacado, ofreciendo la funcionalidad inherente al propio dispositivo. Es el sistema que más se puede asemejar a la definición de un laboratorio de pruebas real, pero, evidentemente con otras misiones encomendadas. El atacante puede obtener un compromiso total de la máquina.
  - *Virtual.* La técnica utilizada es la virtualización (servicios interfaces de conexión, aplicaciones etc.). Es el que más comúnmente se encuentra desplegado entre los sistemas de baja interacción.
- ***Producción.*** Se denominan así por su ubicación junto a la zona de producción real de la organización. Su principal misión es la mitigación por atracción de un posible ataque.
- ***Investigación.*** Su principal objetivo corresponde a la obtención de información de las metodologías y herramientas usadas por los atacantes para que, en paralelo, los investigadores y encargados de la ciberseguridad industrial de la organización, sean capaces de mejorar los sistemas de seguridad y proporcionar ayuda en la hora de toma de decisiones.
- ***Tipo de comportamiento.*** Corresponde a una especialización más de los sistemas HP. Este comportamiento hace referencia a la especialización concreta del sistema a simular (planta potabilizadora aguas, generación energía, procesos químicos, etc.). La situación común es el diseño para un único cometido, puesto que adecuar el honeypot para diferentes

procesos facilita con creces la posibilidad de ser detectado e identificado por los atacantes.

- *Rol de servidor.*

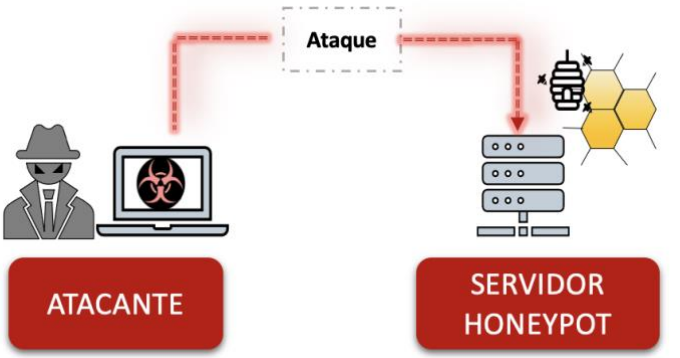


Figura 25: Despliegue básico de un sistema honeypot con el rol de servidor.

Este rol es de un gran interés para las organizaciones, ya que consiste en atraer a los posibles atacantes hacia un entorno seguro y completamente aislado de la organización, captando y registrando todas las acciones llevadas a cabo, y todas las herramientas utilizadas, para a posteriori, realizar un estudio pormenorizado de todas las tareas ejecutadas, y así obtener información que permita una mejor protección. Las premisas que deben cumplir es ser lo más real posible y disponer del software desplegado acorde a las necesidades del entorno industrial simulado. La Figura 25 representa la arquitectura básica de un despliegue de un HP con este rol.

- *Rol de cliente.*

A través de esta funcionalidad, la ejecución del HP se basa en imitar un software que utiliza diversos servicios de un servidor, como por ejemplo disponer de un navegador web altamente vulnerable y ejecutar de forma repetitiva búsquedas y visitas a alojamientos web comprometidos para recibir ataques de estas páginas. Su misión principal es la recopilación de información de las amenazas a las que se

ve expuesto. La Figura 26, representa la arquitectura básica de un despliegue de un HP con el rol de cliente.

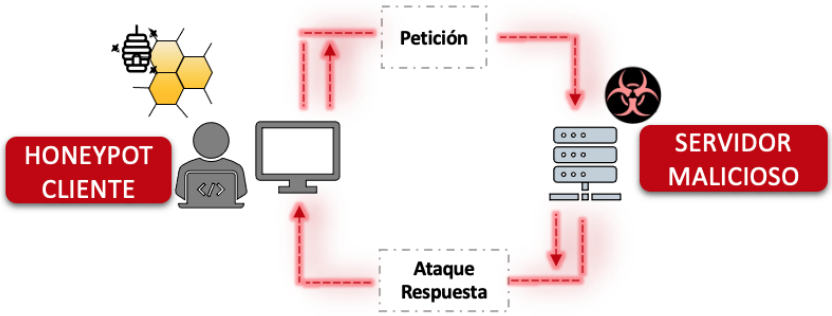


Figura 26: Despliegue básico de un sistema honeypot con el rol de cliente.

- ***Tipo de iteración.*** El tipo de iteración hace referencia a la complejidad y la permisividad que se le otorga al atacante para interactuar con el sistema. A su vez se subdivide en:
  - *Alta interacción*: Estos sistemas se caracterizan por poseer desplegados softwares reales completamente funcionales, como por ejemplo software de ingeniería de programación de PLC y HMI. Aportan mucha información de las metodologías, técnicas y herramientas auxiliares de los atacantes. Es destacable que al ser sistemas y software real deben estar perfectamente securizados y protegidos para evitar que los atacantes puedan realizar movimientos laterales y acceder a otros sistemas ajenos a los honeypots. La Figura 27 representa gráficamente, la arquitectura correspondiente a un sistema de señuelo correspondiente a un sistema de alta interacción.

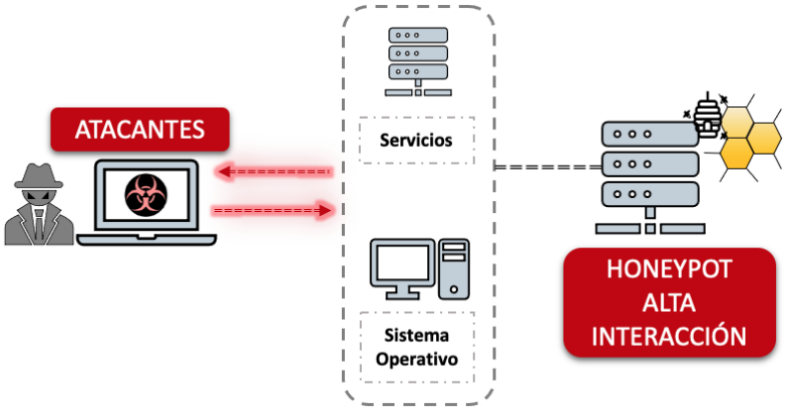


Figura 27: Representación gráfica de una honeypot de alta interacción.

- *Baja iteración* Por contrapartida, los sistemas de baja interacción carecen de tanta complejidad de manejo y despliegue como los de alta. Las aplicaciones instaladas no son totalmente funcionales, facilitando su detección a los atacantes. Ver Figura 28.

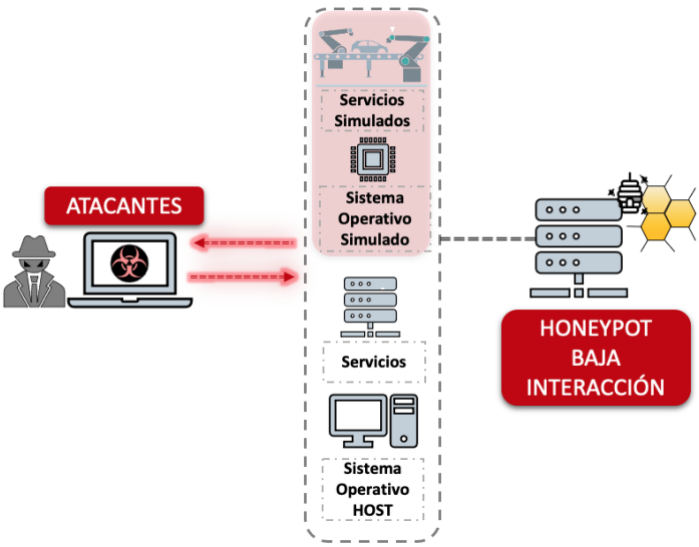


Figura 28: Representación gráfica de una honeypot de baja interacción.

SECTOR AFECTADO	Nº INCIDENTES
Administración	277
Industria nuclear	18
Agua	1922
Energía	151
TIC	724
Transporte	2992
Alimentación	57
Sistema financiero y tributario	1930
Salud	0
Espacio	4
Industria Química	11
TOTAL	8086

Fuente CNPIC

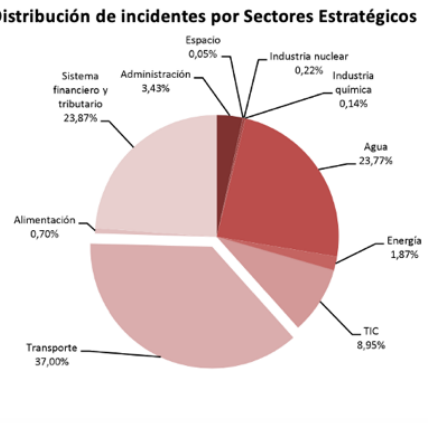


Figura 30: Ciber-incidentes gestionados durante los años 2018-2019, ambos inclusive (fuente: Centro Nacional de Protección de Infraestructuras y Ciberseguridad CNPIC).

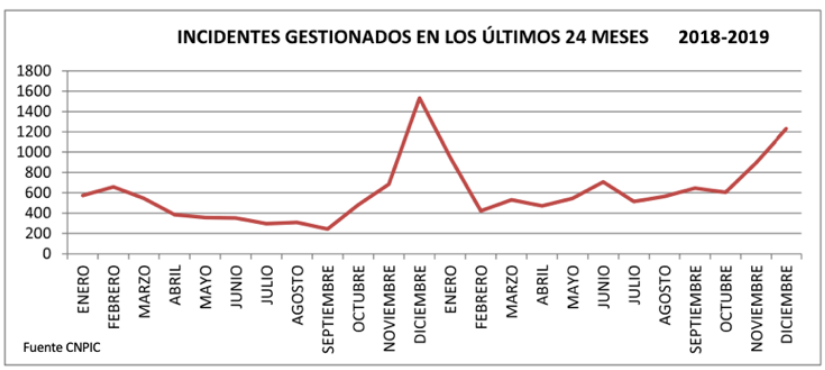


Figura 29: Ciber-incidentes años 2018-2019, ambos inclusive, distribuidos por sectores estratégicos (fuente: Centro Nacional de Protección de Infraestructuras y Ciberseguridad CNPIC).

Como se puede ver en las Figuras 29 y 30, el número de ataques sufridos por los entornos industriales están aumentando en número, frecuencia e intensidad. Estos ciberataques sufridos por los SCI encuadrados en los sectores estratégicos y en infraestructuras críticas pueden llegar a desencadenar una catástrofe de características globales. INCIBE-CERT publicó en abril del año 2020, un informe en el que analiza las tendencias de la ciberseguridad industrial, prediciendo una tendencia al alza de los ciberataques en el sector industrial. El segmento de predicción lo ciñe a la década 2020-2029.

Por este motivo, las predicciones a nivel técnico siguen la línea de las motivaciones descritas en la presente Tesis. Existe una explosión de

dispositivos correspondientes a IITo, conectados para la gestión de dispositivos inteligentes en edificios para su administración, vehículos autónomos, conectividad 5G, etc.

De igual manera y en paralelo, se espera una mayor proliferación de la conciencia y cultura de ciberseguridad apoyada en la detección activa y todo bajo la colaboración nacional e internacional de los Estados, cuyo objetivo será la de compartición del conocimiento y potenciación de la colaboración público-privada [URL- 93, 2021].

3.5. Conclusiones-resumen

A lo largo de este capítulo se ha analizado la situación y el estado de madurez de la ciberseguridad en los SCI, realizando un profundo análisis del estado del arte. Por esta razón, y dada la velocidad con la que los sistemas de control industrial se están viendo influenciados por todo lo relativo a las TI y por su complejidad y diversidad entre TI y TO, el contenido del presente capítulo se ha incrementado considerablemente.

Como consecuencia de la evolución digital y de interconexión a la que se está viendo avocada la industria surgen nuevos escenarios que conllevan ciertas amenazas y, por consiguiente, implican ciertos riesgos. Conocer estos riesgos, así como valorar el nivel de tolerancia dentro de cada organización, no es tarea fácil, máxime por la involucración que poseen los SCI en las infraestructuras críticas. Es por ello que surgen normativas y estándares que vienen a apoyar y legislar estos nuevos paradigmas.

Coexisten, como así ha quedado reflejado en el presente capítulo, numerosas entidades, organizaciones y organismos reguladores que están trabajando en sus respectivos ámbitos, para generar procedimientos que mejoren la ciberseguridad de estos entornos. Estas iniciativas, ya en posesión de un amplio espectro de posibilidades, se encuentran enfocadas hacia la

obtención de información operativa de las últimas técnicas utilizadas por los agentes atacantes. Una de las mejores formas de proteger los sistemas industriales es, en primer lugar, conocer sus propias debilidades y, a su vez, aprender sobre las técnicas de ataques intervenidas y de las cuales han sido objetivo.

Por este motivo, la última sección del presente capítulo ha estado dedicada a los honeypots, puesto que combinados con los laboratorios de pruebas explicados en secciones anteriores conforman una simbiosis perfecta para posicionarse en la mejora de las capacidades de detección y resiliencia.

SICERCAI viene a colaborar directamente en esta área puesto que cumple con cualidades principales como son la capacidad de análisis previo de las infraestructuras y la potenciación de su capacidad de ciber-resiliencia.

Por este mismo motivo, el Capítulo IV está centrado en el desarrollo de una célula de automatización industrial polivalente desplegada dentro de un sistema de TI para la obtención de capacidades de anticipación y resiliencia y para la mejora de la ciberseguridad en el área de la automatización en entornos operacionales. A su vez, el Capítulo V mostrará una investigación concreta y exhaustiva llevada a cabo en redes eléctricas inteligentes y de nueva generación (Smart Grids, por su definición en inglés), donde se realizaron búsquedas de vulnerabilidades de “día 0” en plataformas y dispositivos de los principales fabricantes de sistemas de control industrial a nivel mundial y que se encuentran, a su vez, desplegados en infraestructuras estratégicas/críticas.

Capítulo IV

S.I.C.E.R.C.A.I.

4. Introducción

En el capítulo anterior, se ha detallado el estado actual de todas aquellas partes involucradas en la evaluación, análisis y obtención de propuestas para la mejora de la ciberseguridad de los sistemas de control industrial. En este análisis se han relatado y valorado cuidadosamente todos aquellos medios intervinientes en todas y cada una de sus fases, tanto técnicas como normativas, abarcando esta última la estandarización existente en las comunicaciones y el marco legislativo, nacional, europeo y transfronterizo. A su vez, se han puesto de manifiesto nuevos escenarios acontecidos por la era de la interconectividad, y consecuentemente novedosos sistemas de evaluación y análisis de madurez de los sistemas en materia de ciberseguridad junto a sus dependencias y riesgos asociados.

Como se ha venido indicando a lo largo de los capítulos anteriores, es indispensable desarrollar metodologías cuyos fines sean la identificación de las vulnerabilidades, amenazas y riesgos a los que se encuentran expuestos los SCI y los activos de infraestructuras críticas cualquiera que sea su nivel de complejidad, escalabilidad y heterogeneidad.

Se ha hecho mención especial a las vulnerabilidades emergentes y, por consiguiente, a los nuevos peligros que pueden provocar un estado de ciber-crisis dentro de una organización [URL- 94, 2020]. El concepto de ciber-crisis viene a indicar y contrastar de manera clara, las diferentes etapas en las que un organismo se encuentra expuesto e involucrado desde el momento que forma parte de la industria 4.0.

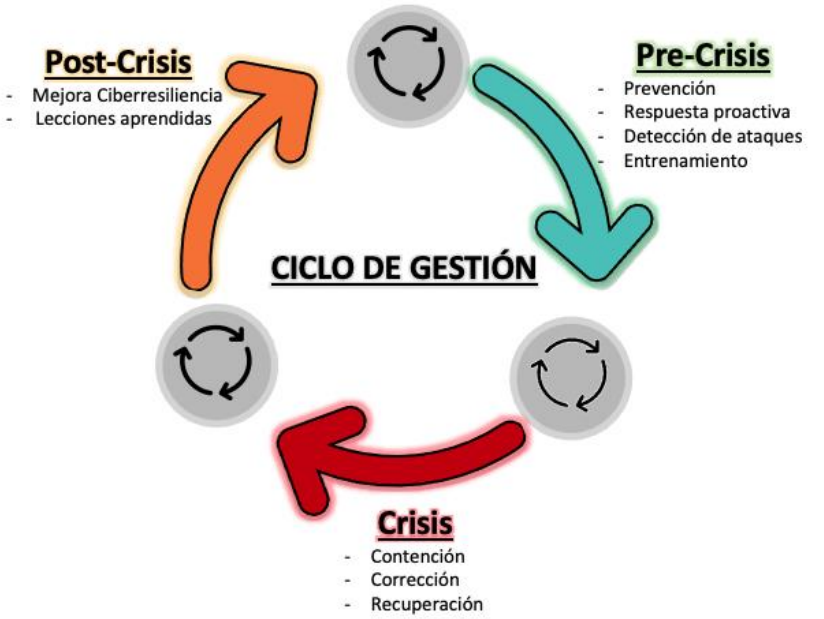


Figura 31: Ciclo de Gestión estado ante una ciber-crisis.

Para ayudar a clarificar el proceso de una manera inequívoca, como así muestra la Figura 31, los estados de una ciber-crisis se pueden clasificar en:

- **Estado de pre-crisis** (corresponde a un estado estable). La organización tiene como objetivo proporcionar todos servicios habituales, realizando acciones preventivas (formación, entrenamiento, concienciación, etc.) incrementando así su capacidad de anticipación ante un posible evento crítico de ciberseguridad. Para esta fase es importante contar con un proceso de gestión de riesgos que permita a la organización pronosticar su aparición y, de esta manera, proporcionar una respuesta proactiva, como así ha quedado detallado en secciones anteriores (por ejemplo, en la Sección 3.3.4.1.).
- **Estado de crisis**. La organización se encuentra bajo una amenaza real como consecuencia de una vulnerabilidad (corresponde a un estado inestable). Las acciones prioritarias a tomar son la contención y recuperación del sistema así como la corrección de la misma.

Se trata de un caso de emergencia en el que es necesario cambiar el enfoque para que las amenazas puedan ser rápidamente eliminadas y sus efectos mitigados.

- **Estado de post-crisis**. La organización debe ejercitar todas aquellas acciones conducentes a la superación de los estados anteriores, con el fin de generar el conocimiento suficiente que dé lugar a las "lecciones aprendidas" como resultado de la fase de crisis, debiendo retroalimentar todos los procesos para reducir y minimizar al máximo los riesgos futuribles (corresponde a un estado estable expuesto a inestabilidad por nuevas amenazas).

Por tanto, en todo el contexto planteado y analizado, SICERCAI proporciona competencias para la mejora de la ciberseguridad, resiliencia, y para la gestión de los estados de crisis a los que se encuentran expuestas las organizaciones, acorde al ciclo de gestión de crisis cibernéticas que se detalla en la sección correspondiente a las propiedades y métricas de los CCI resilientes. De igual manera, es una pieza clave para poder impulsar y colaborar en cada una de las etapas emergentes de una ciber-crisis, aportando conocimiento operativo para su resolución, incorporando las acciones desarrolladas directamente al sistema de gestión de ciberseguridad industrial en cada organización.

Para obtener un resultado real adaptado a las necesidades específicas de la llamada *"evaluación de riesgos previos"* es necesario utilizar escenarios reales. Este tipo de escenarios confieren al mismo tiempo capacidades para la realización de análisis forenses de intervenciones no permitidas y análisis de patrones de comportamiento a través de diferentes herramientas presentes en los sistemas SIEM. Los escenarios recreados a través de SICERCAI tienen la capacidad de pronosticar los efectos que las nuevas amenazas pueden llegar a infligir a los SCI de las infraestructuras críticas.

Por este motivo SICERCAI se postula clave para aportar conocimiento y capacidades preventivas en el estado de pre-crisis, estado inmediatamente previo a una potencial disrupción de la ciberseguridad de los sistemas, confiriendo capacidad de entrenamiento, prevención y detección proactiva en un estado estable de los SCI.

Utilizando el Sistema de Infraestructura del Conocimiento para la Experimentación Real mediante Células de Automatización Industrial, a su vez, se están aportando capacidades para la mejora constante de la ciber-resiliencia, consecuencia ésta de una retroalimentación permanente del conocimiento proporcionado como laboratorio de pruebas.

Durante el transcurso del presente capítulo se procederá a detallar la investigación realizada, verificando las capacidades otorgadas por SICERCAI que han sido descritas como objetivos de la presente investigación.

4.1. Análisis descriptivo de SICERCAI

Como muestra del estudio desarrollado en capítulo previo, los diferentes gobiernos del mundo se encuentran desarrollando planes para la protección de los elementos de sus infraestructuras clave, como son las centrales eléctricas y nucleares, las redes de transporte y de comunicación, los centros de tecnología e investigación, etc.

En paralelo a este creciente interés por la protección de las IC surgen ciertos riesgos para la sociedad, los cuales, a su vez, suscitan irrefutables miedos. Estos son debidos a que las posibilidades de que las interrupciones involuntarias y/o deliberadas hacia las IC aumentan de forma gradual y considerable.

Los factores que propician y refuerzan el reciente aumento del riesgo relacionado con las IC en las últimas décadas se corresponden con:

- *La disminución del control gubernamental* debido a la liberalización y privatización de las infraestructuras. Este punto viene a contrarrestarse en nuestros días por la incipiente colaboración público-privada[62].
- *La proliferación de un uso sin precedentes* de las TIC, las cuales vienen a apoyar, controlar y aportar capacidades de investigación de las funcionalidades de las IC.
- *El asentamiento entre la población de la necesidad* de que los servicios pueden y, sobre todo, deben estar disponibles 24 horas, 7 días a la semana y 365 días al año.
- *El éxodo rural y concentración humana en grandes urbes.* Esto acentúa y pone al límite el uso de antiguas/obsoletas infraestructuras estratégicas/críticas, llevándolas hasta sus niveles máximos de estrés operacional [URL- 95, 2021].
- *La creciente dependencia generada por estas infraestructuras y servicios hacia la sociedad.*
- *Los ciber-delincuentes y ciber-terroristas* que actúan contra la salvaguarda de las IC, convencidos cada vez más de que un ataque exitoso sobre ellas puede causar catástrofes a todos los niveles.

Varias de estas tendencias unidas a los riesgos que conllevan para la sociedad han sido priorizadas por los diferentes Estados para el desarrollo de normativa específica para su protección (detallado en el Capítulo III).

En paralelo, las diversas áreas de investigación existentes en las universidades deciden aportar conocimiento y nuevas vías de exploración enfocadas a la creación de laboratorios (físicos, remotos, virtuales, etc.) para fomentar las capacidades en la mejora de la ciberseguridad y ciber-resiliencia

[62] En España el día 10 de julio de 2020 se constituyó el Foro Nacional de Ciberseguridad, un espacio de colaboración público-privada impulsado por el Consejo de Ciberseguridad Nacional, el cual pretende aglutinar la mayor representación posible de estos organismos.

de estos sistemas de control. Estas iniciativas tienen en la actualidad muy buena acogida entre los estamentos públicos y privados debido a la transparencia, independencia e innovación colaborativa con las empresas.

España es un país altamente implicado en la ciberseguridad de las IC y que a su vez destaca por su constante adaptación de la normativa en esa materia [LEY PIC, 2011]. Así por ejemplo, la Orden PCI/487/2019 de 26 de abril por la que se publica la Estrategia Nacional de Ciberseguridad 2019, [URL- 96, 2019], en su Línea de Acción 5ª, respondiendo al Objetivo IV de la Estrategia, proclama la necesidad de *"… Potenciar la industrial española de ciberseguridad y la generación y retención de talento…* …impulsando programas de apoyo a I+D+I en seguridad digital y ciberseguridad en pymes[63] (pequeñas y medianas empresas), empresas de ámbito internacional, universidades y centros de investigación…"

Por este último motivo, y remarcando el posicionamiento y el trascendental papel que tienen los centros de investigación junto a las universidades, todo ellos deben tomar la iniciativa en la provisión de escenarios para la realización de pruebas de simulación y ensayos de componentes reales de la industria, así como de las arquitecturas desplegadas para este fin. La importancia de los entornos virtualizados debe quedar relegada a un segundo plano, puesto que los sistemas industriales requieren contextos reales con una completa disponibilidad operativa. Estas acciones pretenden generar confianza en el mundo de las TO [Cendoya A., 2016], [Resilience Team ENISA, 2016], [Resilience T. ENISA (a), 2016].

[63] Es el acrónimo para pequeña y mediana empresa, que incluye a todas aquellas empresas con menos de 250 trabajadores y una facturación anual inferior a 50 millones de euros.

Otra motivación base que asiste a la justificación y motivación del trabajo que aquí se presenta, se corresponde con el análisis del informe técnico "Introducción al marco de certificación de componentes de ciberseguridad" (Introduction to the Framework Certification of Cybersecurity Components, ICCF, por sus siglas en inglés) [European Commission, 2016 y 2019], publicado por el servicio de ciencia y conocimiento de la Comisión Europea (Joint Research Center, JRC, por sus siglas en inglés). Este informe tiene como objetivo proponer un conjunto inicial de requisitos comunes y exhaustivos para promover la certificación de ciberseguridad de los sistemas de control industrial en Europa, hasta el punto de que los proveedores están estimulando nuevas demandas respondiendo con innovación en sus productos para idear la certificación de ciberseguridad de los componentes de los Sistemas de Automatización y Control Industrial (SACI).

La aplicación de este requerimiento de exigencias desarrolla un papel clave en la protección de las infraestructuras críticas, propiciando como resultado la mejora de la resiliencia de los sistemas y, por lo tanto, una mayor sensación de seguridad para los ciudadanos. Se incrementa así la cadena de valor en los procesos.

El marco de certificación de ciberseguridad de los componentes de los SACI, (ICCF) pretende proporcionar la ayuda suficiente para que la certificación en ciberseguridad sea fluida y sencilla, siempre a un coste controlado y con reconocimiento dentro y fuera de las fronteras europeas.

De este modo, es factible la posible inclusión del sistema SICERCAI como una arquitectura más que colabore en la mejora de la ciberseguridad y ciber-resiliencia de los SACI, teniendo cabida por su propia naturaleza dentro del papel de ICCF, identificado como laboratorio, y cumpliendo con

las vías de tasación consistentes en la evaluación, la valoración, el ensayo y la certificación.

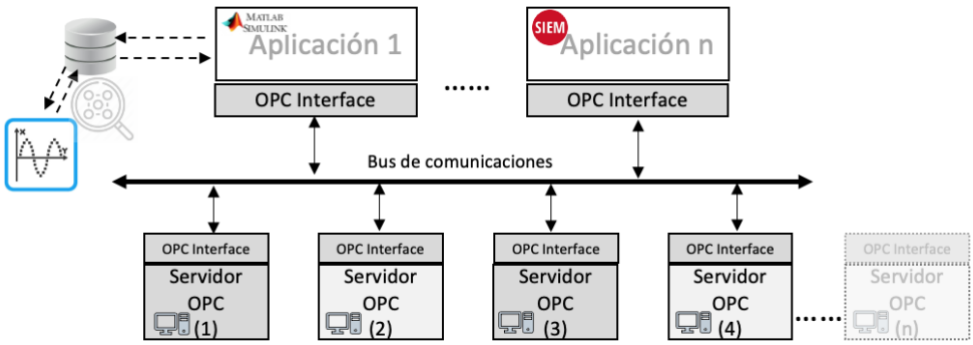


Figura 32: Representación gráfica de conexión con estructura cliente-servidor (OPC).

En la Figura 32 se detalla de forma gráfica las modalidades de conexión [Chiza L., 2021], [SINEMA R.C., 2020]. Estos elementos de la red pueden ser interconectados con MATLAB y Simulink [URL- 97, 2021], [Math W., 2020], obteniendo de esta forma patrones de comportamiento en diferentes entornos industriales recreando:

- *Simulación de procesos ininterrumpidos en el tiempo y de forma totalmente automática* (señales continuas y discretas).
- *Simulación de procesos discretos*, en función de los datos aportados por agentes externos (sensores analógicos y digitales, terminales remotos, etc.).

Diseño de controladores proporcionales, integrales y derivativos (Proportional Integral Derivative Control, PID, por sus siglas en inglés) como mecanismos de control por retroalimentación, típicos de un PLC.

Figura 33: Célula de Automatización Industrial C.A.I.-1.

La Figura 33 se corresponde con la Célula de Automatización Industrial CAI-1 desarrollada como herramienta básica para este estudio. Se ha realizado empleando una arquitectura de componentes y SACI del fabricante SIEMENS. Con esta CAI se ha podido implementar a nivel atómico cada uno de los procesos más comunes y existentes en cualquier entorno industrial. Los elementos industriales incorporados en el CAI-1 proporcionan diversas capacidades que se llevan a cabo en los procesos industriales [Marcos M., 2004].

Los PLC SIEMENS S7 1200, principales elementos industriales incorporados en la CAI-1, son utilizados a través de un servidor que utiliza el estándar de comunicación con arquitectura cliente servidor (Ole for Process Control, OPC, por sus siglas en inglés, representada en la Figura 32).

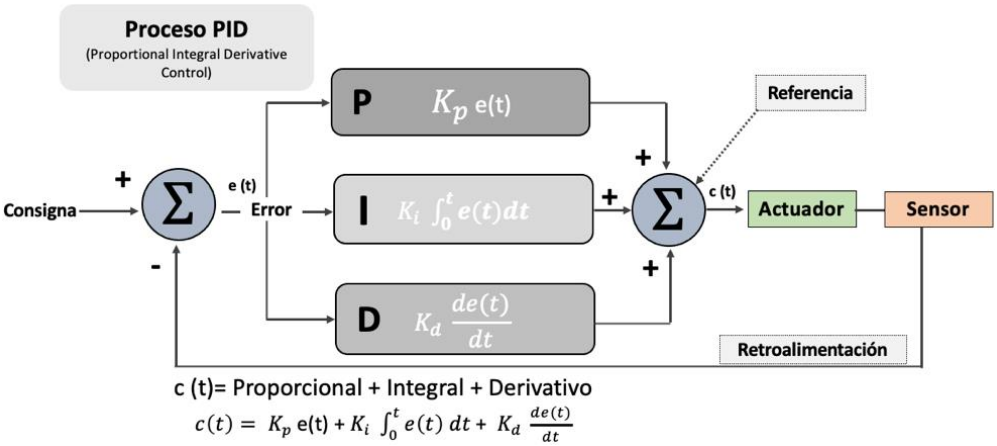


Figura 34: Diagrama de bloques de un controlador proceso proporcional integral y derivativo (PID) realimentado.

- La Figura 34 describe matemáticamente las etapas intervinientes en un controlador proporcional, integral y derivativo [Chekari T., 2021].
- *Análisis de patrones gráficos obtenidos de los procesos*.
- *Conectividad local y remota bajo arquitecturas multiplataforma*, confiriendo la capacidad de analizar vulnerabilidades asociadas a SCI, sistemas operativos y, lo que es más importante, la casuística de la combinación de ambos.
- *Despliegue de sistemas SIEM* no sólo asignados a las TI sino también a las TO [Sarno C., 2016], [James R., 2019], [Setola R., 2016].

En resumen, lo que esta investigación trata de determinar es la eficacia de la predicción al conocer las medidas preventivas adoptadas y, como consecuencia directa de ello, aprender a mejorarlas y corregirlas con la suficiente anterioridad [Elhady M., 2019], [Upadhyay D., 2019].

4.2. Importancia de la protección y ciber-resiliencia en SACI

Hasta este momento, se han estado precisando cuestiones dirigidas a los actores involucrados en los desarrollos de las áreas TI y TO sobre la problemática emergente y acechante a los SACI, haciendo partícipe a los diferentes estamentos que se encuentran involucrados en la protección de las IC (públicos, privados, técnicos, nacionales, internacionales, etc.).

No obstante, la cuestión más interesante que se debe remarcar y tener muy en cuenta es por qué se debe aumentar el interés por la protección y la resiliencia de estos sistemas.

Como se ha detallado anteriormente, entre la sociedad se encuentra asentada la necesidad de que los servicios proporcionados por las IC tienen la obligatoriedad de mantenerse disponibles para nuestro beneficio de forma permanente. Esta reflexión involucra directamente de forma global a todos los Estados.

De hecho, como ha quedado descrito inicialmente, así como por numerosas razones económicas, sociales, políticas y tecnológicas [Luiijf H., 2010], este desencadenamiento de acciones ha provocado una vertiginosa variación en los aspectos organizativos, operativos y técnicos de las infraestructuras críticas. Estas IC, que en el pasado podían considerarse sistemas autónomos integrados verticalmente con muy pocos puntos de contacto con otras infraestructuras, ahora están estrechamente ensambladas y muestran un gran número de dependencias transversales. Esto ha generado abundantes efectos positivos para nuestra sociedad, pero ha aumentado la complejidad, la vulnerabilidad de las infraestructuras y por consiguiente el riesgo para nuestro estado del bienestar. Varios episodios de ciberataques han sido registrados en las dos últimas décadas y han puesto

de relieve esta fragilidad, siendo éstos recogidos en el tercer capítulo de esta memoria. Aunque los ejemplos de incidentes listados poseen grandes diferencias en términos de causas primarias, extensión y consecuencias, todos ellos se caracterizan por dependencias no intuitivas y, sobre todo, por medidas de protección inadecuadas para gestionar la crisis. Esto se debe principalmente a la falta de comprensión de un evento y especialmente de sus consecuencias directas e indirectas [Adamas K., 2011]. Esto es, por desgracia, un efecto de la creciente complejidad del escenario socio-técnico[64] caracterizado en gran medida por la presencia de dependencias entre diferentes IC.

La Figura 35 viene a representar las dependencias de ámbito transversal ante la clasificación de los tipos de fallos.

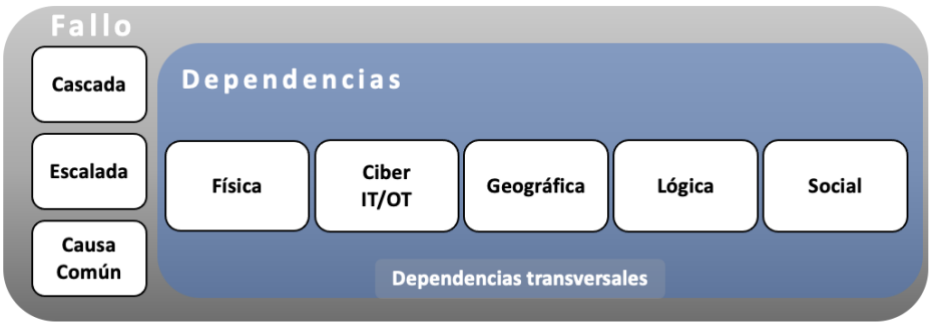


Figura 35: Representación gráfica de dependencias de ámbito transversal.

4.3. Propiedades y métricas de los SCI resilientes

En otra revisión de los conceptos de resiliencia utilizados para las IC, Riccardo Patriarca y Alessandro De Apolis en [Riccardo P., 2021], presentan un modelo de simulación en el que se combinan métricas sencillas que se

[64] La definición de socio-técnico fue acuñado por los investigadores F.E. Emery y E.L. Trist en 1953, siendo designado para la identificación de la iteración obrero-máquina en los ambientes de desarrollo industrial.

centran en la resiliencia del sistema a nivel técnico, observando la evolución y comportamiento de éste.

En el estudio llevado a cabo por Francis R. Y Bekera [Francis R., 2014], estos autores concluyen que las definiciones que componen la ciber-resiliencia parecen converger *" hacia una misma dirección de una definición tradicional, ya que estas definiciones comparten varios elementos comunes; capacidad de absorción, capacidad de recuperación capacidad de adaptación y conservación de la identidad (estructura y funciones)".* Mantienen que el objetivo de la resiliencia es conservar las dimensiones predeterminadas del sistema, funcionamiento y la identidad o la estructura del sistema en vista de los escenarios previstos. Por lo que aparecen definidas tres capacidades de la resiliencia: *absorción, adaptación y restauración*. Estas cualidades aparecen íntimamente relacionadas con las distintas etapas del ciclo típico de respuesta de las infraestructuras ante las perturbaciones (antes, durante y después del evento disruptivo).

En el mismo estudio relatado anteriormente [Francis R., 2014], se definen las siguientes capacidades de resiliencia de las infraestructuras:

- ***Capacidad de absorción*.** Se refiere al grado en que un sistema puede asumir los impactos de las perturbaciones hacia el mismo y minimizar las consecuencias con un esfuerzo reducido. En este concepto se encuadra a su vez el nivel de tolerancia que una organización asume o está dispuesta a afrontar en caso de una disrupción en sus servicios. En la práctica, sin embargo, es una característica de gestión que depende de la configuración, los controles y los procedimientos operativos. La solidez y la fiabilidad del sistema son características prototípicas previas a las perturbaciones de un sistema resiliente.
- ***Capacidad de adaptación.*** Mientras que la capacidad de absorción es la capacidad de un sistema para asumir y tolerar las perturbaciones del

sistema, la capacidad de adaptación es la medida de un sistema para ajustarse a situaciones no deseadas mediante algunos cambios automáticos o manuales. La capacidad de adaptación de un sistema se ve reforzada por su capacidad para anticiparse a los acontecimientos imprevistos, de reorganizarse después de un acontecimiento adverso y de estar prevenido en general para los eventos adversos.

- ***Capacidad de restablecimiento.*** Esta cualidad de un sistema resiliente suele caracterizarse por la rapidez de retorno a la normalidad o la mejora del funcionamiento y la fiabilidad del sistema. Esta capacidad debe evaluarse en función de un conjunto definido de requisitos derivados de un nivel de servicio o control deseado.

En la Figura 36, se pueden ver claramente definidas y representadas las capacidades de resiliencia y estados que marca una disrupción en un sistema.

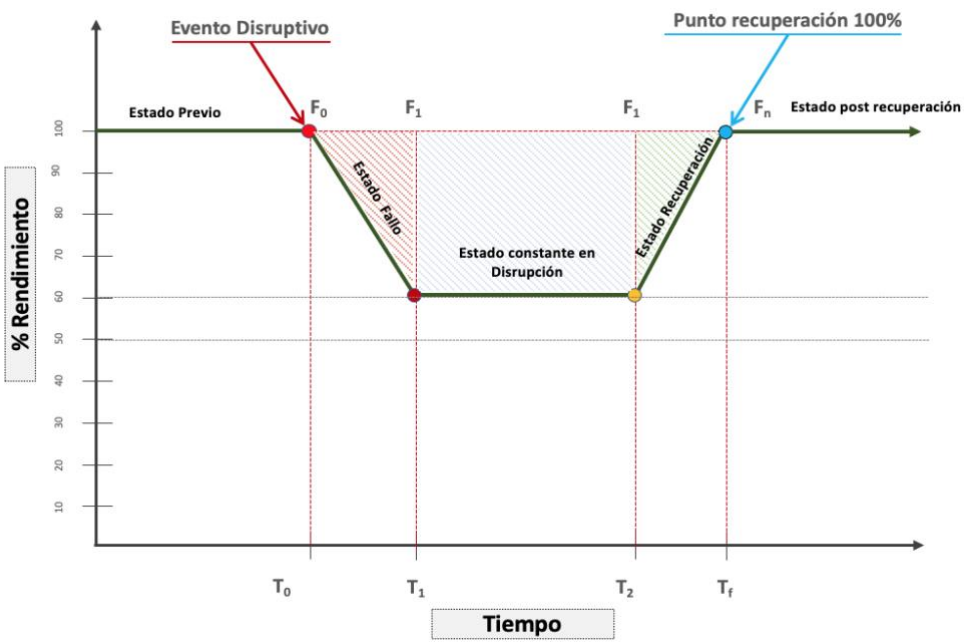


Figura 36: Gráfica representativa de las capacidades de resiliencia y estados ante una disrupción.

Siguiendo el modelo planteado en [Riccardo P., 2021], y considerando la descripción de resiliencia y sus capacitaciones previas, la capacidad de la absorción, (Abs) puede ser obtenida como la relación del rendimiento residual con respecto al original, en el mismo instante en el que se produce el evento disruptivo, es decir;

$$Abs = \left(\frac{F_1}{F_0}\right) * F_{env} \qquad \text{Expresión (8)}$$

Donde F_{env} se corresponde con el factor de envejecimiento.

F_0 y F_1 se corresponden con el rendimiento original y el rendimiento residual, respectivamente.

$$F_{env} = 1 + \left(\frac{F_0 - F_1}{F_0}\right) \qquad \text{Expresión (9)}$$

El factor de envejecimiento es igual a 1 si se parte de la hipótesis de que no existe un efecto de envejecimiento, siendo F_0=F_1.

La medida de la capacidad de adaptación, (Adp) está definida por el intervalo de tiempo en el que el sistema alcanza un nuevo estado estable después del fallo y lo mantienen hasta el momento en el que las acciones de recuperación entran en acción para restablecer el sistema:

$$Adp = 1 - \left(\frac{T_2 - T_1}{T_f - T_0}\right) \qquad (10)$$

Cuanto mayor sea el tiempo existente entre las operaciones de recuperación (es decir, cuanto mayor sea la diferencia $T_f - T_0$), menor será la capacidad de adaptación del sistema.

La medida de la capacidad de recuperación se define como la pendiente de la curva de recuperación en comparación con la pendiente de recuperación lineal ideal de 90◦.

$$RtAct = \frac{\text{Arctan}[\frac{F_n - F_1}{T_f - T_2}]}{\frac{T_f - T_0}{90}} * R_t \quad (11)$$

$$R_t = \frac{T_2 - T_0}{T_f - T_0} \quad (12)$$

Donde

Rt, Indica el factor de tiempo se recuperación lineal.

La medida final de resiliencia se obtiene a través de la siguiente relación booleana que implica las capacidades de absorción, restauración y adaptación del sistema:

$$Res = Abs \vee (Adp \wedge Rst) \\ = Abs + [(Adp * Rst) - (Abs * Adp * Rst)] \quad (13)$$

Donde Res *= Resiliencia,* ***Abs*** *= Absorción,* ***Rst*** *= Restauración* ***Adp*** *= Adaptación.*

La capacidad que tiene un sistema para la absorción se asume como una cualidad independiente. A diferencia de la adaptación y la recuperación, no es reactiva sino que es un propiedad sistémica del medio [Rioshar Y., 2021].

Una mayor capacidad de absorción se traduce en un impacto menos significativo sobre otras capacidades y, en consecuencia, menores esfuerzos y recursos requeridos tras la disrupción. Una mayor capacidad de adaptación indica mayores niveles de rendimiento tras el evento disruptivo. La puntuación obtenida para la resiliencia (*Res)* es, por tanto, una medida comprendida entre los valores 0 y 1, que sigue siendo significativa, especialmente para las comparaciones relativas entre diferentes configuraciones de los sistemas.

Según la perspectiva arrojada en [Francis R., 2014], afirma que es importante tener en las interdependencias inherentes, y que existen entre la

mayoría de las IC modernas, un esquema claro de la composición de elementos que integran las capacidades de resiliencia.

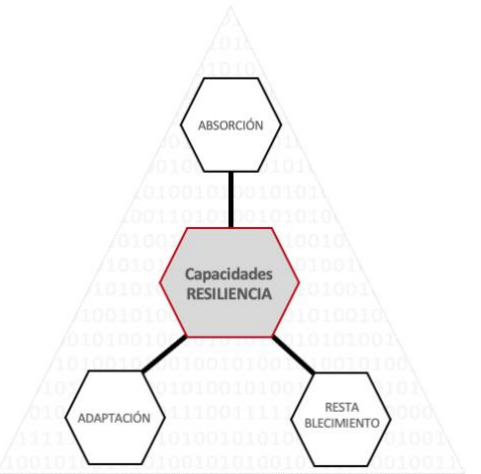


Figura 37: Componentes involucrados en la resiliencia.

En este sentido, los conceptos y medidas de resiliencia propuestos deben incorporar las dependencias de las IC, considerando la caída en cascada provocada por algún fallo de alguna o múltiples IC, que ofrecen diferentes servicios a la comunidad [Eeten M., 2011], [Warnier M., 2017]. Esta dependencia de la resiliencia entre los sistemas y las infraestructuras ha sido reconocida en la literatura científica [Alheib M., 2016]. En la Figura 37 se describe gráficamente los componentes que integran parte de la cualidad de ostentar peculiaridades de resiliencia, y que a su vez influyen de manera independientemente en la globalidad de su comportamiento.

Como se destaca en [Kamran M., 2020], la resiliencia es el concepto emergente que viene a ayudar a mitigar las pérdidas causadas por desastres cibernéticos en particular. Puede desempeñar un papel importante para la mejora sostenida del sistema si se preserva y promueve el patrimonio cultural necesario para crear conciencia sobre ella.

La evaluación de la resistencia de las infraestructuras proporciona atributos clave en todas las fases, es decir, antes, durante y después de la catástrofe. Si estos atributos se abordan correctamente, resulta fácil fomentar la resiliencia de las infraestructuras. SICERCAI se encuentra presente en todas las fases descritas en la resiliencia.

En resumen, la dimensión proporcionada en esta sección se refiere principalmente a las propiedades físicas de los componentes de la infraestructura, sistemas, redes o "sistemas de sistemas" y se centra en las características y comportamiento de éstos en caso de cambio o incidente. Esta dimensión es muy importante cuando se refiere a la resiliencia de la ingeniería de los SCI.

En general, un enfoque basado en la resiliencia para las IC debe corresponderse con una visión holística del problema y que, gradualmente, se debe ir adoptando por los Estados y demás actores implicados en las IC.

Esto redundará directamente en los beneficios proporcionados por ser capaces de hacer frente a los retos y los costes para lograr la máxima protección en un entorno cada vez más complejo. Consiguiendo así superar las limitaciones de un enfoque tradicional de gestión de riesgos basado en escenarios en el que la organización puede carecer de capacidades para afrontar el riesgo de amenazas y vulnerabilidades desconocidas o imprevistas.

4.4. SICERCAI Metodología, materiales y análisis

Tras haber detallado en el tiempo la evolución, y en paralelo la exposición que se está produciendo en materia de ciberseguridad en los SACI desde sus orígenes, se ha puesto de manifiesto que estos sistemas se encuentran comúnmente desplegados en IC, cuya desprotección y operación malintencionada influye directamente en la sociedad.

Ha quedado remarcada la importancia que supone mantener inquebrantable la disponibilidad de estos sistemas, primando la capacidad de reforzar y potenciar su seguridad para así potenciar la capacidad de resiliencia.

Como ya se comentó en la introducción, esta investigación se ha llevado a cabo en un área muy concreta: la ciberseguridad industrial. Específicamente, proporciona un valor diferenciador ante este concepto y su aplicabilidad en el sector de los servicios esenciales [Sarry A., 2016], [Wang S., 2016].

Por estos motivos en esta sección se refleja el estudio explícito llevado a cabo en un área específica, basada en la capacidad de mejora de la ciberseguridad en sistemas de control especializados en la automatización de procesos.

La arquitectura especificada así como los pasos llevados a cabo para cumplir con los objetivos establecidos se ha desarrollado de forma modular y en diferentes etapas. Como se detalla en la descripción de los objetivos de esta investigación, ha sido necesario considerar, desde un punto de vista global, la unión de los mundos de las TI y de las TO, otorgando la misma importancia a ambos. Como consecuencia del concepto de la CTIO se explora una nueva forma de experimentar en el campo de la ciberseguridad industrial, creando un sistema con características destacables ante las capacidades de cohesión que posee y su versatilidad de configuración para los requerimientos que se propongan como premisas para la ejecución de las mismas [Ross R., 2016], [Roldán G., 2017].

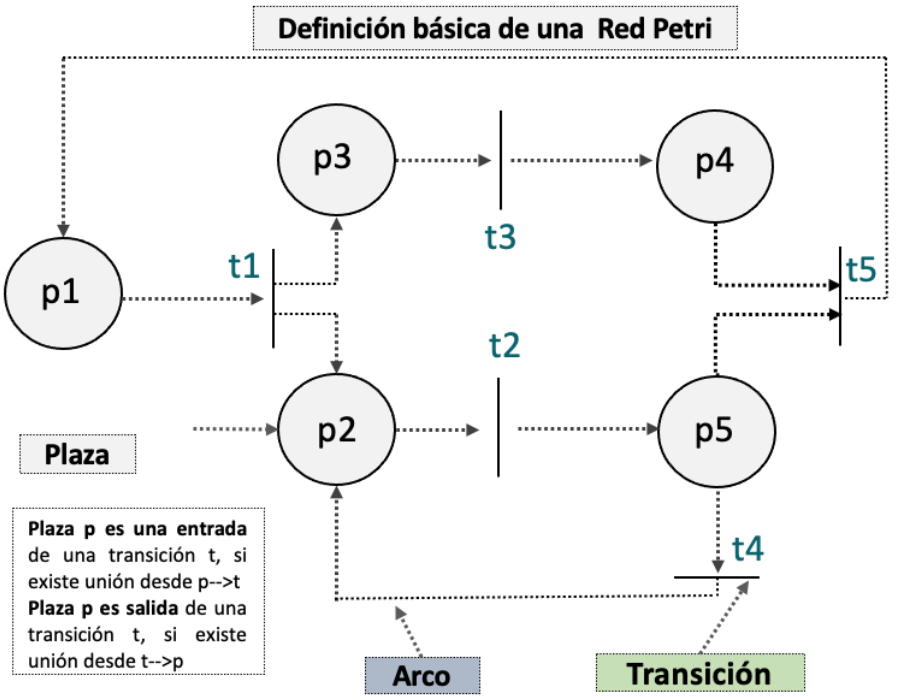


Figura 38: Definición básica del modelado de una Red Petri.

La investigación presentada se ha concretado con el despliegue y la programación de un sistema de control de tráfico rodado [González S., 2020], utilizando y definiendo su comportamiento a través de una red de Petri[65] [Kochkin D., 2020].

Este modelado matemático de comportamientos, como se describe en la Figura 38, viene a cubrir la representación de un sistema distribuido de un conjunto de transiciones que afectan a los elementos de una red de control de tráfico para obtener un resultado real y adaptado a las necesidades específicas de la conocida *"evaluación de riesgos previos"* en un sistema de gestión a través de autómatas programables.

La convergencia entre las TI y las TO debe implicar el campo tecnológico y la definición más pura de los procesos mecánicos, electrónicos

[65] Una red de Petri es un grafo orientado con dos tipos de nodos: lugares y transiciones.

y electromecánicos soportados por la intercomunicación de los mismos. Esta situación viene a plantear la necesidad de la obtención de los objetivos específicos planteados en el Capítulo 2 de esta Tesis.

Así SICERCAI viene a dispensar las capacidades de:

- ***Evaluación*** de la eficacia de una arquitectura específica de TO y TI.
- ***Aplicabilidad*** de diferentes patrones de comportamiento bajo la creación de medios de modulación y evaluación.
- ***Portabilidad*** de la célula de automatización para una rápida conectividad fuera del ámbito de los laboratorios remotos y virtuales.
- ***Capacitación*** sobre la alta cualidad de cohesión con tecnologías de diferentes *fabricantes.*
- ***Proporcionar*** la capacidad de desplegar cualquier sistema operativo cuya misión sea interactuar con el laboratorio y estaciones de ingeniería.
- ***Suministro*** de capacidades de análisis en tiempo real de las vulnerabilidades de SO de en un sistema de control industrial y, lo más interesante, de ambos al mismo tiempo.
- ***Facilitación de protocolo de comunicación ante el descubrimiento*** de alguna vulnerabilidad del tipo "0 Day" que se encuentre durante las ejecuciones. El protocolo de notificación requeriría un acuerdo confidencial previo entre la universidad y el fabricante del dispositivo industrial a ensayar, que se renovaría cada dos años o cuando cambiaran las condiciones que originaron este acuerdo [URL- 98, 2019].

❑ ***Obtención de patrones*** de comportamiento de diferentes fuentes:

- Patrones de comportamiento obtenidos del sistema SIEM de AlienVault [URL- 99, 2021] (Open Source Security Information Management, OSSIM por sus siglas en inglés).

- Bases de datos mostradas en el sistema de control y adquisición de datos, (Supervisory Control and Data Acquisition, SCADA por sus siglas en inglés).
- Patrones gráficos generados a partir de diferentes variables industriales.

- **Generación de cultura de ciberseguridad** extrapolable al mundo académico, siendo el punto de partida las infraestructuras críticas y fabricantes de dispositivos industriales españoles y europeos.

4.5. Nivel de contribución e innovación de SICERCAI

Como se ha descrito en secciones anteriores, esta memoria presenta la creación de una célula de automatización industrial con diferentes componentes procedentes del mundo de las TO y que, a su vez, forma parte de un sistema con otras capacidades de banco de pruebas principalmente del mundo de las TI (Figura 33).

Esta composición permite al sistema abordar la investigación sobre la ciberseguridad de las CTIO para la mejora de la ciber-resiliencia. Como punto de referencia para el análisis y desarrollo de este trabajo se ha tomado como criterio normativo el estándar procedente de ISA99/IEC62443 (ver Figura 39). Este estándar constituye el marco principal de referencia internacional para su aplicación en la ciberseguridad de los sistemas industriales donde es de vital importancia mantener la disponibilidad e integridad de estos.

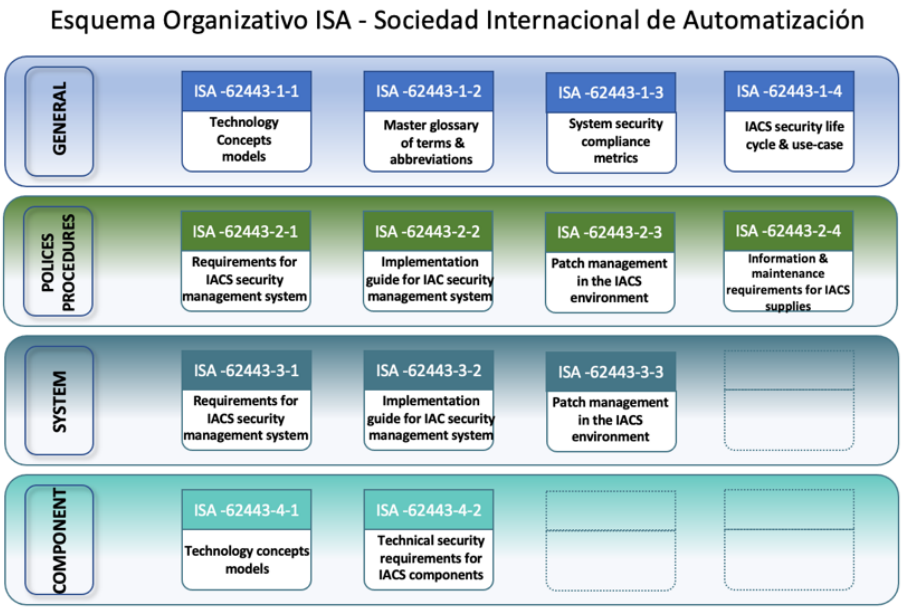


Figura 39: Esquema organizativo según la Sociedad Internacional de Automatización (modificada de la fuente original: ISA).

Estos factores se han tenido en cuenta básicamente para la adopción de medidas de protección contra las amenazas cibernéticas, pero también para la reducción de los incidentes tecnológicos involuntarios. Esto se sustenta en los diferentes apartados de la norma IEC 62443 y particularmente en las secciones detalladas en la Figura 39. La información aquí descrita representa un avance en el campo del análisis de riesgos.

La miscelánea en el mundo real de estos componentes de software y hardware sería imposible de simular mediante el concepto clásico de un laboratorio virtual de acceso a distancia, como se expone en la introducción. Así pues, se ha dado un paso adelante en el tratamiento correcto de dos ámbitos muy diferentes, que requieren la convergencia de las tecnologías de control e información en el sector.

Hasta el momento, estas dos tecnologías habían seguido caminos paralelos según lo dictado por los avances industriales y tecnológicos. El capítulo introduce un nuevo concepto que enriquece el nivel de madurez de la ciberseguridad que puede considerarse como un método de defensa en

profundidad, a saber, "el conocimiento a través de la experimentación real" [González S., 2020]. Este nuevo concepto contiene percepciones que lo diferencian de las que tradicionalmente se suponen mediante el uso de accesos remotos y/o laboratorios virtuales. Los verdaderos laboratorios de acceso remoto no siempre están disponibles para las necesidades que puedan surgir. Este hecho es evidente y difícil de resolver, ya que no existen plataformas que faciliten todas estas posibilidades de arquitecturas desplegadas en el mundo de la producción industrial. La posibilidad de proceder a recrear estas configuraciones en SICERCAI a través del servidor de máquinas virtuales admite infinitas combinaciones funcionales sin tener que buscar configuraciones similares en laboratorios remotos, independientemente del tipo de acceso que se tenga implementado, lo que cambia el concepto estático de las arquitecturas de otro banco de pruebas.

De esta forma, se ayuda a desterrar el temor que rodea a los sistemas operativos de la industria en relación con su idoneidad en el campo de la ciberseguridad. Además, ofrece la posibilidad de experimentar en un entorno controlado con dispositivos complejos dada su funcionalidad, dando respuesta a preguntas como:

- *¿Qué sucedería si el sistema operativo se actualizara desde el entorno operativo?*
- *¿De cuánto tiempo se dispone para hacer una parada programada para bajar las actualizaciones de seguridad?. ¿Seguirá todo igual?*
- *¿Es posible una actualización de emergencia en los sistemas industriales en producción?*
- *¿Es realmente consciente de las posibles amenazas a sus sistemas de control industrial?*

4.6. Transferibilidad

Como se ha informado en secciones anteriores, SICERCAI se ha diseñado fundamentalmente para aumentar las capacidades de anticipación y resiliencia en los entornos de las diferentes infraestructuras desplegadas en los SACI.

Es importante subrayar que los entornos de pruebas y verificación en los sistemas de control industrial son altamente demandados por entidades que poseen IC, ya que no disponen de suficiente capacidad para la realización de testeos previos, que indiquen y pronostiquen los posibles comportamientos inherentes a las actualizaciones del sistema en alguno/s de sus componentes o arquitecturas.

Estas características están directamente relacionadas y clasificadas por los niveles de criticidad de sus acciones, de ahí la importancia de crear un sistema capaz de proporcionar estas medidas de previsión ante el suceso de posibles eventos disruptivos. Asimismo, la Comunidad Europea viene a tutelar las acciones encaminadas hacia los esfuerzos para la obtención y asentamiento de un sistema de certificación para aumentar la ciber-resiliencia de las IC (ICCF). En consecuencia, sería provechoso tener en cuenta a SICERCAI como elemento a incluir como banco de pruebas en los sistemas críticos existentes en los 12 sectores estratégicos definidos por la Ley Española [LEY PIC, 2011], [Real Decreto 704, 2011].

4.7. Arquitectura de SICERCAI

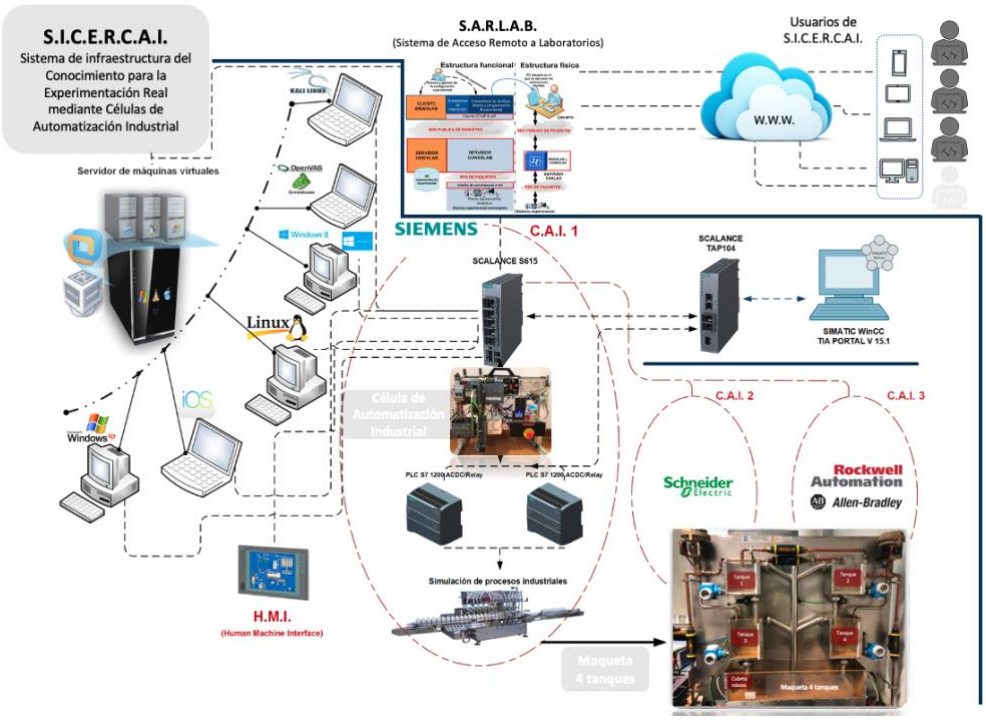


Figura 40: Gráfico correspondiente al Sistema de Infraestructura del Conocimiento para la Experimentación Real mediante Células de Automatización Industrial. - SICERCAI-©

La Figura 40 describe el entorno creado para proporcionar las capacidades de prueba a los sistemas industriales. La arquitectura representada está compuesta de varios subsistemas.

El acceso se gestiona mediante el Sistema de Acceso Remoto a Laboratorios (SARLAB) [Sánchez M., 2015], el cual proporciona acceso a un servidor de máquinas virtuales que facilita de ejecución de diferentes sistemas virtuales que se ponen a disposición de los usuarios, y que pueden ser configuradas de acuerdo con los objetivos previstos a alcanzar y evaluar. Esto proporciona una vía real de usabilidad de las diversas células de automatización industrial existentes, permitiendo su gestión mediante el uso de una interfaz hombre-máquina. Esta arquitectura incluye todos los componentes resultantes de la CTIO creados en esta investigación.

Además, permite el desarrollo y la evaluación de las diferentes arquitecturas planteadas a distancia por la comunidad de usuarios y provee acceso de forma controlada y ordenada a la comunidad que utiliza el sistema, al tiempo que el conocimiento generado por las distintas combinaciones de instrucción puede ser extrapolado al mundo académico, así como a las infraestructuras críticas españolas y europeas y a los fabricantes de dispositivos industriales.

4.7.1. Subsistema SARLAB

Como así se define por Sánchez Márquez en su Tesis Doctoral [Sánchez M., 2015], *SARLAB* se encuentra implementado sobre la familia de protocolos TCP/IP, que son los más utilizados en Internet y en la inmensa mayoría de redes internas o intranets.

Para apoyar la labor de la gestión las comunicaciones para la materialización de una sesión formativa en remoto, *SARLAB* proporciona acceso a una sesión práctica de un laboratorio remoto (ASPLR, Access Session Practice Laboratory Remote). Como ayuda y así poder establecer de forma transparente las conexiones requeridas para la configuración de las diferentes pruebas, limitando el número de túneles de comunicación que faciliten las conexiones necesarias entre el PC del alumno y el sistema experimental se dispone de *CONEXLAB* (*CON*exión *EX*periencias al *LA*boratorio). De igual manera *SARLAB* cubre el control del flujo de datos entre el usuario conectado a través de Internet y la experiencia a desarrollar (conexión de la red local de la entidad o ubicación de la entidad que la proporciona), siendo aquella la ubicación física de la CAI a utilizar. Esta cualidad la proporciona la portabilidad de las CAI.

Las funciones de gestión del laboratorio (altas, bajas y modificaciones de los roles de usuarios y grupos) se asocian a una nueva funcionalidad

denominada *DIGEXLAB* (*Diseño y Gestión para EXperiencias de LABoratorio*), que se encargará de tramitar las estructuras matriciales de configuración de las experiencias correspondientes a un laboratorio de acceso remoto.

Así, *DIGEXLAB* gestiona la base de datos de representación experimental. En la Figura 41, se representa la introducción a las dos estructuras representadas a través de *CONEXLAB* y *DIGEXLAB* mediante una estructura cliente-servidor.

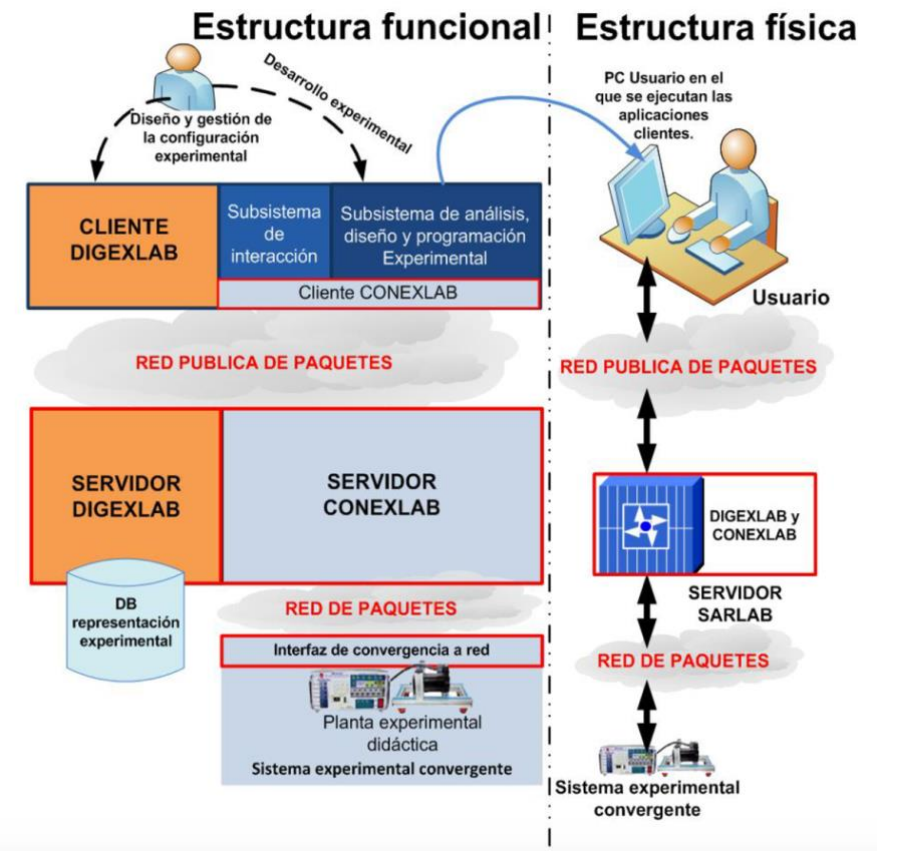


Figura 41: Representación gráfica de la estructura funcional de SARLAB (CONEXLAB-DIGEXLAB).

SARLAB, a su vez, es responsable de la gestión de la concurrencia permitida para cada tipo de experiencia requerida, proporcionando, además, capacidades de accesos colaborativos.

La Figura 42 describe de una manera gráfica, cómo se produce la interacción de *CONEXLAB*.

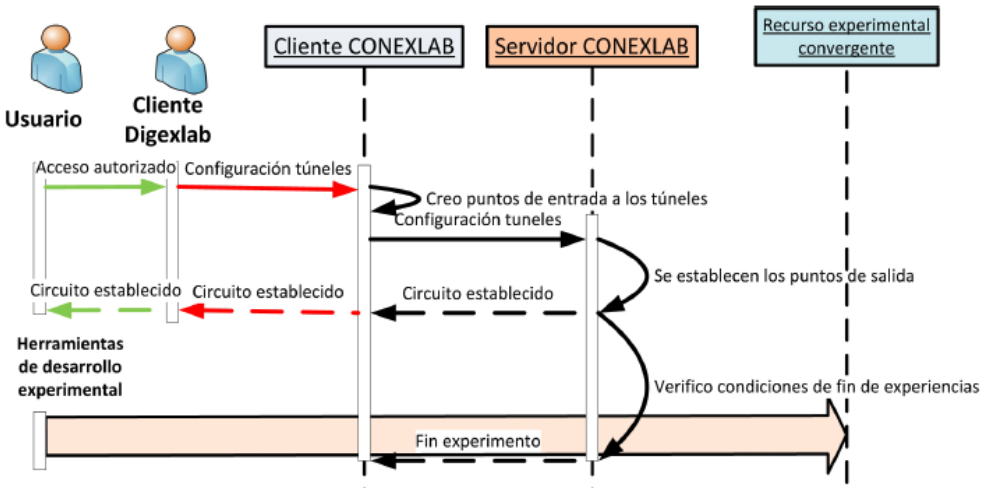


Figura 42: Descripción de la interacción de CONEXLAB.

4.7.2. Servidor de máquinas virtuales

Como se ha detallado en el gráfico general de la arquitectura de SICERCAI, (Figura 40), se ha desplegado un servidor con capacidad de albergar diferentes máquinas virtuales (MV) habilitando la posibilidad de desplegar nuevas instancias de ellas. Estas MV están a disposición de los usuarios según la necesidad de su utilización. La Figura 43, parte del sistema completo, incorpora una descripción gráfica del servidor de máquinas virtuales [URL- 100, 2021].

Este sistema de virtualización está basado en la utilización de un software, el cual va a permitir generar réplicas perfectas de un recurso tecnológico físico. Este recurso, en el caso en particular descrito en esta Tesis, se corresponde con máquinas de computación con diferentes sistemas operativos.

Para profundizar en el conocimiento de esta funcionalidad y su práctica a través de SICERCAI, se deben clarificar varios conceptos.

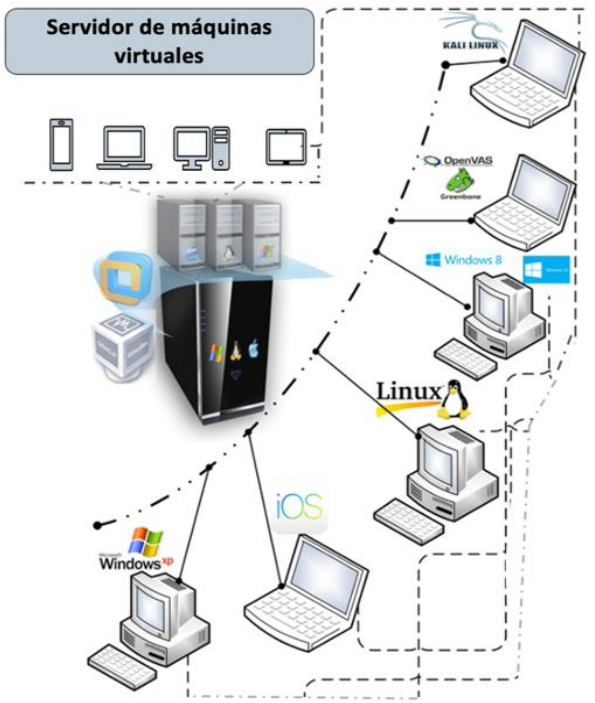


Figura 43: Disposición de servidor de máquina virtuales a disposición de los usuarios.

Por definición y adjudicación de funciones, el servidor físico encargado de realizar las veces de anfitrión de soporte del software de virtualización es el denominado host. Para el caso que nos ocupa y en la Sección 4.7.3., se describen expresamente las características técnicas del servidor ESXI virtualizado con VMware, sobre el que se han instalado varias máquinas y sistemas operativos para el análisis de comportamiento y necesidades técnicas en pre-producción para, a posteriori su pase a producción en un cluster habilitado en el Departamento de Informática y Automática de la UNED. La funcionalidad básica del host es al alojamiento de los recursos a virtualizar, conocidos como máquinas virtuales (Virtual Machines, VM, por sus siglas en inglés), a través del software de virtualización elegido para tal fin. Este software puede corresponder a dos clases diferentes: nativo y/o alojado.

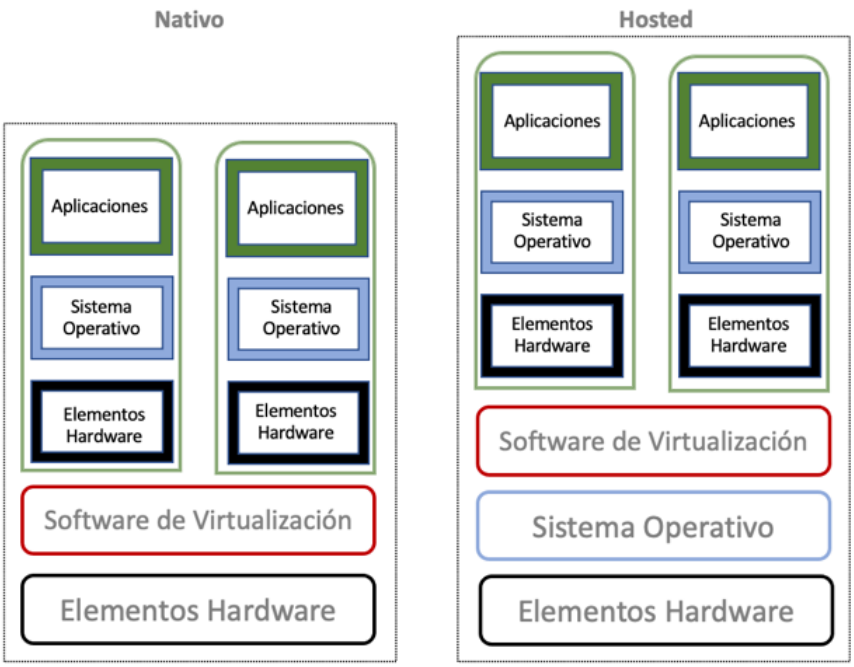


Figura 44: Diferenciación entre modos y sistemas de virtualización.

El software nativo destaca porque el software de virtualización realiza a la vez las funciones de sistema operativo, ejecutándose directamente del host o anfitrión. Mientras que el software alojado se ejecuta sobre el SO del host. La Figura 44 representa la arquitectura funcional de cada tipo.

El *software* de virtualización es el encargado de llevar a cabo la simulación de los recursos de hardware ineludibles para cada máquina virtual. Por ello y para cada uno de estos sistemas que se desea virtualizar, hay que definir diferentes aspectos individualmente. Estos se corresponden con: la memoria principal (Random Access Memory, RAM por sus siglas en inglés), unidades de DVD, almacenamiento y capacidad de disco, procesador, etc.

La cantidad de recursos que consumirá una VM nunca podrá ser superior a la que requiere el software de virtualización para ser ejecutado.

Actualmente los tipos de software más utilizados para el desarrollo y configuración de máquinas virtuales son:

- ***Oracle Virtual Box.*** [URL- 101, 2021]. Oracle VM VirtualBox se corresponde con un software de virtualización capaz de operar en arquitecturas x86/amd64[66]. Actualmente es desarrollado por Oracle Corporation como parte de su porfolio de servicios de virtualización. Utilizando este software se está en posesión de la capacidad de instalar sistemas operativos adicionales, conocidos como **«sistemas invitados»** dentro de otro sistema operativo **«anfitrión»**, y cada uno con su propio contexto virtual. Entre los sistemas operativos soportados (en modo anfitrión) se encuentran GNU/Linux, Mac OSX, OS/2 Warp, Genode, Windows y Solaris/OpenSolaris, y, a su vez, internamente a ellos es posible virtualizar los sistemas operativos FreeBSD, GNU/Linux, OpenBSD, OS/2 Warp, Windows, Solaris, MS-DOS, Genode y muchos otros. VirtualBox ofrece algunas funcionalidades interesantes, como la ejecución de máquinas virtuales de forma remota a través del protocolo de control remoto utilizado (Remote Desktop Protocol, RDP, por sus siglas en inglés), soporte iSCSI[67], aunque estas opciones no están disponibles en la versión libre de código abierto (Open Source Edition, OSE, por sus siglas en inglés). Referente a la emulación de los componentes de hardware, los discos duros de los sistemas invitados son recolectados en los sistemas anfitriones como registros individuales emplazados en un contenedor denominado "*Virtual Disk Image*". Dispone de capacidades de emulación de controladores de aceleración en 3D, pantalla completa, hasta 4 placas PCI Ethernet (8 si se utiliza la línea de comandos para configurarlas), integración con teclado y ratón. Desde la versión 6.0, VirtualBox ya no es

[66] La familia x86, agrupa los microprocesadores compatibles con instrucciones Intel 8086. Amd64, popularmente conocido como x86_64 y AMD64, es la versión de 64 bits del conjunto de instrucciones x86.

[67] iSCSI, Internet corresponde a un estándar para el uso del protocolo SCSI, que es un protocolo de capa transporte, sobre redes TCP/IP.

compatible con sistemas operativos anfitrión de 32 bits, pero sí se pueden crear máquinas virtuales tanto de 32 bits como de 64 bits.

- ***VMware.*** [URL- 102, 2021]. VMware Inc. es una filial de EMC Corporation (propiedad a su vez de Dell Inc.) que provee software de virtualización para computadores compatibles con arquitecturas X86. Este software está compuesto por VMware Workstation, VMware Server y VMware Player, siendo estos dos últimos de carácter gratuito. El software de VMware puede ser ejecutado en dispositivos anfitriones con SO Windows, Linux y en la plataforma MacOS con procesadores de arquitectura Intel, y bajo el nombre de VMware Fusion. Se corresponde con un sistema que permite operar con software, emulando a un sistema físico, al igual que VirtualBox (un computador, un hardware, etc.) con unas peculiaridades de hardware determinadas. Cuando se ejecuta el programa (simulador) provee un ambiente de ejecución similar a todos los efectos a un computador físico (excepto en el puro acceso físico al hardware simulado), con CPU (puede ser más de una), BIOS, tarjeta gráfica, memoria RAM, tarjeta de red, sistema de sonido, conexión USB, disco duro (pueden ser más de uno), etc. Un virtualizador por software permite ejecutar (simuladamente) diversos terminales dentro de un mismo hardware de manera concurrente, permitiendo así la mayor explotación de recursos. Sin embargo, al ser una capa intermedia entre el sistema físico y el sistema operativo que funciona en el hardware emulado, la velocidad de ejecución de este último es sensiblemente menor, pero en la mayoría de los casos suficiente para ser ejecutado en entornos de producción. VMware es equivalente a su homólogo VirtualBox, aunque existen divergencias entre ambos que perturba la forma en la que el software interactúa con el sistema físico. El rendimiento del sistema virtual varía en función de las características del sistema anfitrión en el

que se ejecute, y de los recursos virtuales (CPU, RAM, etc.) asignados a cada máquina virtual. Una de la ventajas principales que se deben tener en cuenta a la hora de elegir un software u otro, es que mientras que VirtualBox emula una plataforma x86, VMware la virtualiza de forma que la mayor parte de las instrucciones en VMware se ejecutan directamente sobre el hardware físico, mientras que en el caso de VirtualBox se traducen en llamadas al sistema operativo que se ejecuta en el sistema físico.

En la Tabla 15 se relacionan otras alternativas para la creación de entornos virtuales, así como un enlace para su explicación y acceso a la descarga.

Otras alternativas de software de virtualización	
KVM	https://www.redhat.com/es/topics/virtualization/what-is-KVM
SLM Galeon	http://www2.slm.cloud/
Hyper-V	https://hipertextual.com/2017/01/hyper-v-maquina-virtual-microsoft
Promox VE	http://911-ubuntu.weebly.com/proxmox_como_funciona/conoce-como-funciona-proxmox-y-como-usarlo
Xen	https://cloud.ibm.com/docs/virtualization?topic=virtualization-what-is-citrix-xenserver-&locale=es
Virtual PC	https://support.microsoft.com/es-es/topic/descripci%C3%B3n-de-windows-virtual-pc-262c8961-90e5-1125-654f-d87cd5ba16f8
BOCHS	https://ubunlog.com/bochs-una-alternativa-open-source-a-virtualbox-llega-a-su-version-2-6-10/
QEMU	https://sites.google.com/site/virtualizaciongt/home/maquinas-virtuales/Qemu
Virtuozzo	https://cloud.ibm.com/docs/virtualization?topic=virtualization-what-is-virtuozzo-&locale=es
Basilisk II	https://basilisk.cebix.net/
SheepShaver	https://sheepshaver.cebix.net/
FlexVM	**HTTPS://DOCS.FORTINET.COM/PRODUCT/FLEX-VM/1.0**

Tabla 15: Relación de diferentes alternativas de virtualización existentes en el mercado.

Al utilizar los entornos de virtualización, estos permiten ser generados a través de varias vías y con diferentes opciones. Gracias a ellos se tiene la capacidad de virtualizar servidores al completo: almacenamiento, redes de

comunicación, aplicaciones, entornos de trabajo individuales, etc. En el caso de SICERCAI se han virtualizado diferentes sistemas operativos, los cuales corresponden a los que se pueden encontrar en los entornos industriales actualmente existentes.

La versatilidad del sistema por el que se ha optado viene a otorgar capacidades dinámicas y adaptabilidad en el tiempo, basándose en el momento concreto del entorno industrial que sea necesario evaluar.

Como se ha puntualizado en el Capítulo 3 de esta Tesis, hoy en día existen SO desplegados en los entornos operacionales con una obsolescencia ya superada y completamente carentes de coberturas de soporte técnico por parte del fabricante, encontrándose expuestos a todo tipo de vulnerabilidades. Por este motivo, el subsistema que proporciona la elección y puesta a disposición del usuario del tipo de SO virtualizado en SICERCAI, es de suma importancia por su capacidad de adaptación a los requerimientos base, correspondientes al sistema a evaluar por el usuario.

Basándose en las necesidades planteadas por los usuarios de SICERCAI, el servidor proporciona la capacidad de hacer uso de un determinado número de máquinas virtuales y la posibilidad de actuar con diferentes SO. Los SO se clasifican en tres categorías según la funcionalidad que ofrecen dentro de SICERCAI:

- ***Pentesting***.

  Un *pentesting* es un conjunto de ataques simulados dirigidos a un sistema informático con una única finalidad: detectar posibles debilidades o vulnerabilidades para que sean corregidas y no puedan ser explotadas de manera malintencionada.

- ***Sistemas de producción***.
- ***Sistemas de programación y adquisición de conocimientos.***

  Dentro de la funcionalidad de pentesting, los SO disponibles son:

- *Sistema OpenVAS*[68], el cual facilita la creación de scripts de evaluación y búsqueda de vulnerabilidades de dispositivos industriales.
- *Kali Linux,* que dispone de varias herramientas de auditoría de red.
- *SamuraiSTFU,* que se corresponde con un sistema de auditoría específico para entornos industriales.

Para los sistemas de producción existen varias versiones de sistemas operativos Windows (por ejemplo, la 7 y la 10) que soportan un amplio abanico de posibilidades relacionadas con el funcionamiento de los sistemas según la programación de sistemas de entornos industriales utilizando WinCC[69], así como la simulación de redes corporativas como parte integrante de las redes industriales en producción.

También se extiende a los sistemas de producción en las DMZ[70] analizando los posibles fallos de seguridad derivados de las vulnerabilidades del sistema operativo, las arquitecturas de red o los sistemas de programación de PLC [URL- 32, 2019].

[68] OpenVAS es una herramienta de código abierto que realiza escáneres en busca de vulnerabilidades, que proporciona varios servicios y herramientas, proporcionando una solución completa y poderosa para la administración y gestión de vulnerabilidades.

[69] *SIMATIC WinCC* es un sistema de control de supervisión y adquisición de datos e interfaz hombre-máquina de Siemens.

[70] En las redes informáticas, una DMZ (zona desmilitarizada) es una subred física o lógica que separa una red de área local (LAN) interna de otras redes que no son de confianza, normalmente Internet.

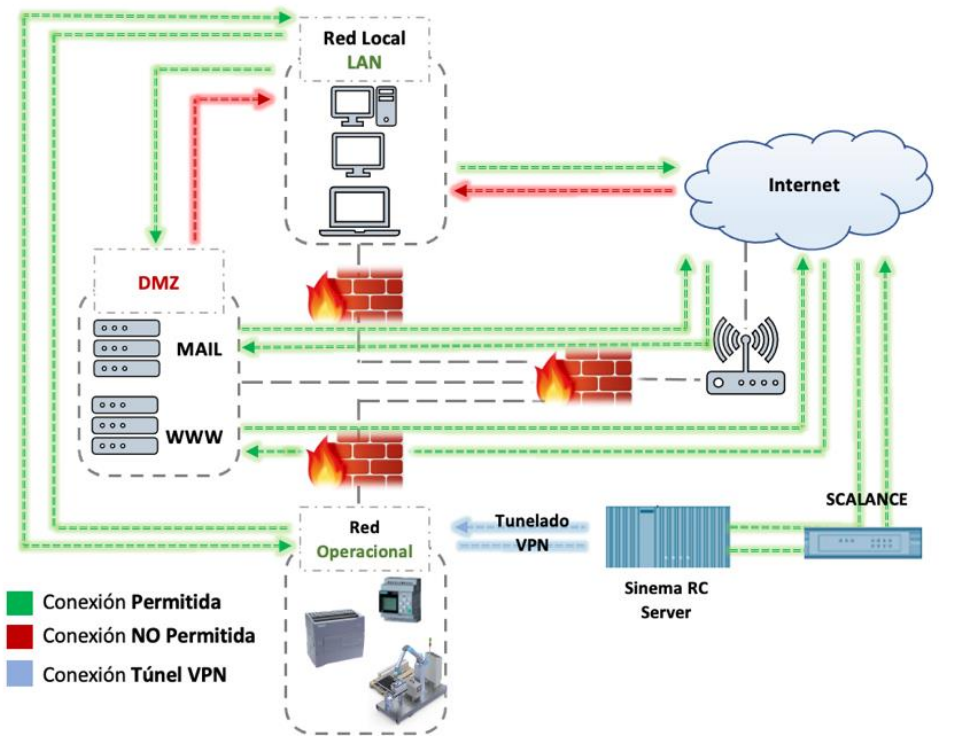


Figura 45: Gráfico representativo, posible modelo de red con diferentes servicios y modos de acceso.

La Figura 45 detalla un posible modelo arquitectónico de conexión tras una correcta segmentación de redes dentro de cada organización teniendo en cuenta sus particularidades. Se han representado la red de gestión (red local), la red operacional y la DMZ.

A su vez, en SICERCAI existe un sistema SCADA desarrollado mediante un WinCC flexible V8 que recoge los datos producidos en la red industrial recreada. Al mismo tiempo, hay una estación de ingeniería con el software TIA Portal [URL- 103, 2021], (Totally Integrated Automation Portal), cuya misión es proporcionar la capacidad de los programas de PLC y otra instrumentación utilizada en OT.

4.7.3. Características técnicas del servidor de MV

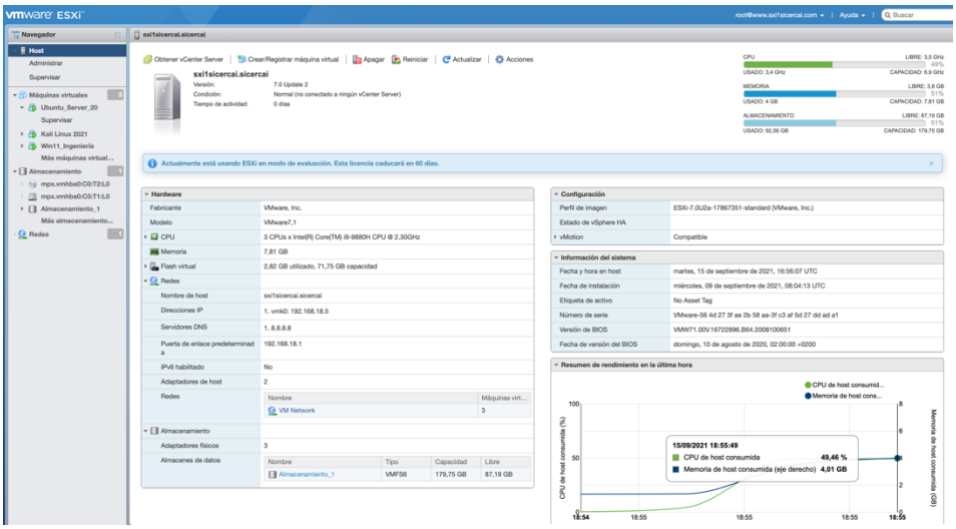


Figura 46: Características técnicas del servidor ESXI virtualizado con VMware.

La Figura 46 se corresponde con la característica principal del servidor ESXI desplegado en fase de pre-producción para su posterior despliegue en el cluster habilitado al efecto en el Departamento de Informática y Automática de la UNED.

Para poder llevar a cabo una migración a posteriori, con plenas garantías a un entorno de producción, se ha procedido a virtualizar el servidor sobre un sistema vmware ESXI versión 7.0, el cual contiene tres máquinas virtuales que se corresponden con los siguientes SO:

- *Kali Linux.* Esta máquina proporciona herramientas de auditoría sobre el sistema desplegado.
- *Windows 11.* Este sistema operativo soporta las herramientas de ingeniería para la programación y configuración de los autómatas (TIA Portal en su versión 15.1).
- *Ubuntu Server v. 20.* Este sistema operativo proporciona capacidades para poder desplegar sobre él servicios como los comentados en secciones

anteriores (herramientas de tunelación VPN, Sinema Remote Connect, etc.).

En la Figura 47 se muestran los datos correspondientes a la CPU, memoria y almacenamiento del entorno en donde se ha virtualizado en Vcenter para gestión del ESXI (fase de pre-producción).

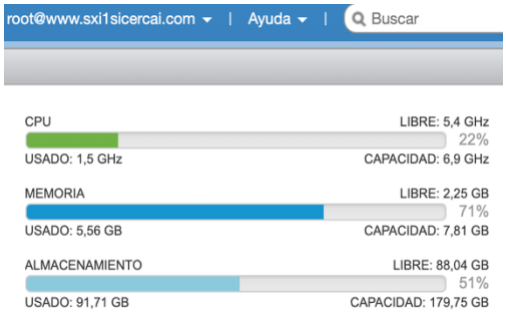


Figura 47: Gráfico representativo de los recursos de hardware utilizados por el servidor ESXI.

La Figura 48 se corresponde con un gráfico resumen del rendimiento de host en donde se ha procedido a virtualizar el servidor de máquinas virtuales, en un momento determinado. Este tipo de gráfico ayudan a evaluar comportamientos como consecuencia de las pruebas de estrés a las que se somete al servidor ESXI, para garantizar unas características mínimas de hardware para ser configurado en un entorno de producción.

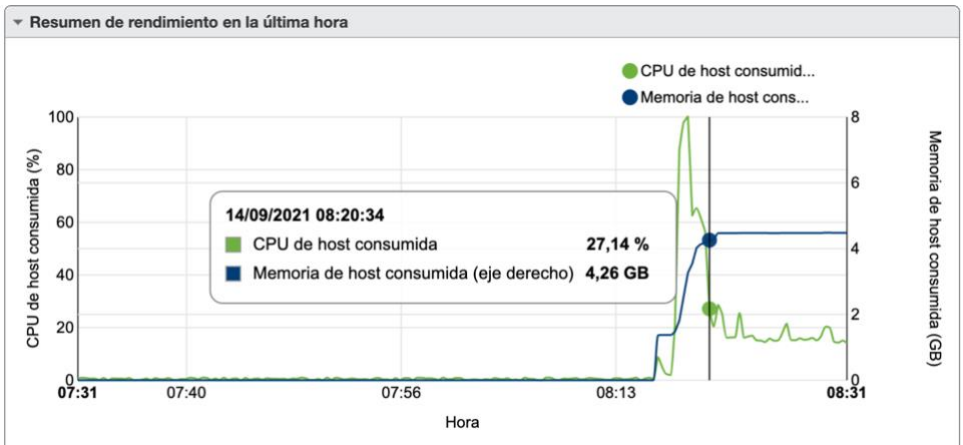


Figura 48: Gráfico representativo del rendimiento del host donde se encuentra desplegado el servidor ESXI.

A continuación se muestran las máquina virtuales desplegadas en el servidor ESXI así como sus características técnicas principales.

- *Ubuntu Server* (Figura 49)

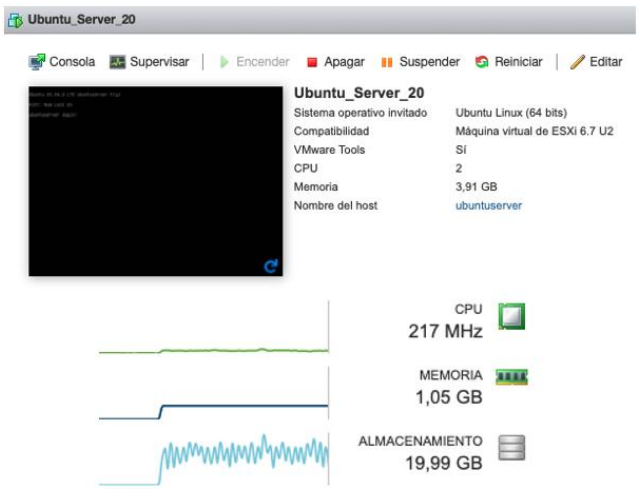


Figura 49: Características principales de la máquina virtual Ubuntu creada en el ESXI.

- *Windows 11* (Figura 50)

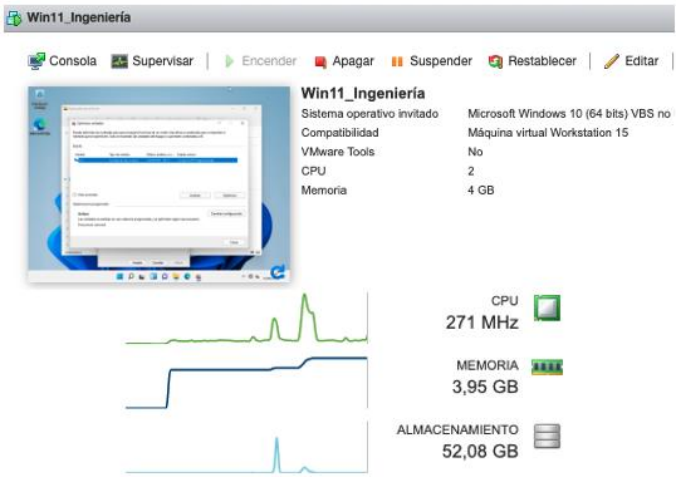


Figura 50: Características principales de la máquina virtual Windows 11 creada en el ESXI.

- Kali Linux 2021 (Figura 51)

Figura 51: Características principales de la máquina virtual de auditoría Kali Linux 2021 creada en el ESXI.

4.8. Célula Automatización Industrial (CAI)

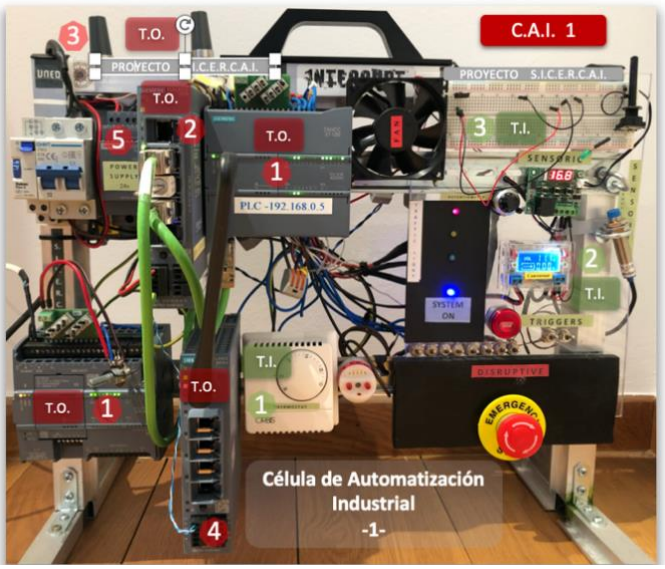


Figura 52: CAI-1 con identificación de cada componente incorporado de TO y TI.

En esta subsección se van a describir, de manera individualizada, los componentes de la célula de automatización industrial creada, detallando la funcionalidad de cada uno de ellos.

En primera instancia se ha considerado una CAI única con instrumentación de SIEMENS. Los componentes de la CAI, de aquí en adelante denominada CAI-1, y el banco de pruebas industrial diseñado se relacionan en la Tabla 16 y quedan identificados en la Figura 52.

La estructura ha sido montada sobre una plataforma de dimensiones 55cmx50cmx30cm. Esta arquitectura desde el principio se proyectó como esencial, puesto que la tecnología operacional así desplegada, proporcionaría una fácil portabilidad y adhesión en cualquier laboratorio de pruebas.

Familia de los componentes		Núm.	Componente
T.O.	**Corresponde en CAI con instrumentación industrial TO**	1	**PLC SIMATIC S7-1200** CPU 1214C AC/DC/RLY, una placa de disparo, capaz de actuar directamente sobre la circuitería del PLC proporcionando acceso manual a sus entradas digitales
			SCALANCE S615 INDUSTRIAL ROUTER
		3	**SCALANCE W778-1 M12** SIMATIC NET IWLAN Access Point
			SCALANCE M876-4 INDUSTRIAL MODEM & ROUTER
		5	**LOGO POWER** 100-240v DC24v
T.I.	**Corresponde en CAI con elementos pertenecientes a TI**		**TERMOSTATO** Analógico de temperatura
		2	**ELEMENTOS SENSORIALES** Voltímetro/conversor; sonda digital temperatura, detector electromagnético, potenciómetros, pulsadores de emergencia
			PLACA DE PRUEBAS 840Tie 2Bus Strips

Tabla 16: Identificación de componentes de la CAI-1, de la parte TO y TI.

4.8.1. PLC SIMATIC S7 1200 -1214C AC/DC/RLY

Como se puede apreciar en la Figura 52, la CAI-1 está dotada de dos controladores lógicos programables de la gama S7 1200. Se ha optado por estos dispositivos en concreto, puesto que la gama S7-1200 abarca distintos tipos de controladores lógicos programables (PLC) que pueden utilizarse para la mayoría de las tareas desarrolladas en la automatización industrial. La Figura 53, se corresponde con los dos controladores lógicos programables instalados en la CAI-1.

Figura 53: PLC S7 1200, instalados en la CAI-1.

Los modelos de los PLC se corresponden con el S7-1200, 1214C, AC/DC/RLY, y el software de programación que se ha utilizado para su programación ha sido el TIA Portal[71] V15.1, software basado en Windows, el cual ofrece la flexibilidad suficiente y necesaria para solucionar las tareas de automatización y virtualización propuestas en esta Tesis.

La unidad central del controlador incorpora un microprocesador, una fuente de alimentación integrada, circuitos de entrada y salida, un bus PROFINET integrado, E/S de control de movimiento de alta velocidad y entradas analógicas incorporadas, todo ello en un chasis compacto, conformando así un potente controlador. Además, dispone de un puerto de comunicaciones tipo RJ-45 para conexiones TCP/IP.

Una vez cargado el programa en la CPU, ésta contiene la lógica necesaria para vigilar y controlar los dispositivos de la aplicación. La unidad central vigila las entradas y cambia el estado de las salidas según la lógica del

[71] TIA Portal corresponde a un paquete completo de software, propietario de SIEMENS, cuya misión es proveer soluciones de automatización optimizando los procesos de ingeniería.

programa del usuario, que puede incluir lógica booleana[72], instrucciones de contaje y temporización, funciones matemáticas complejas, así como

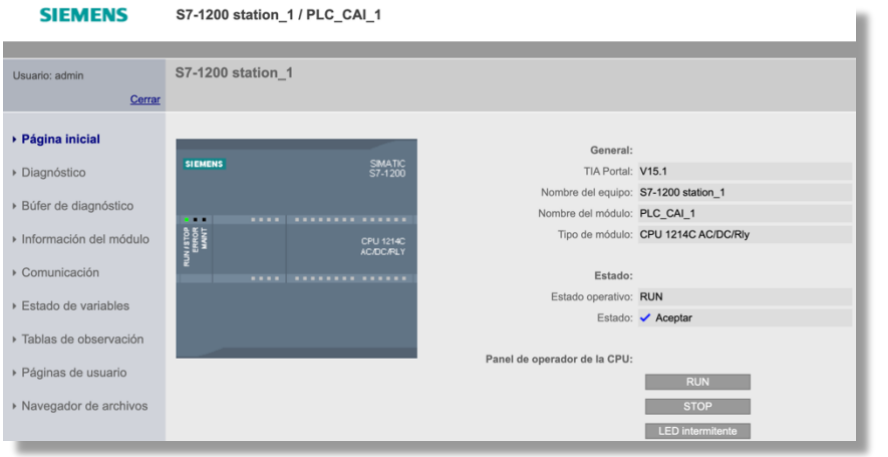


Figura 54: Pantalla de configuración de el servidor web del PLC S7-1200.

comunicación con otros dispositivos inteligentes.

La Figura 54 muestra la pantalla de acceso al PLC desplegado en SICERCAI mediante la conexión vía TCP/IP al servidor web del controlador.

Es importante destacar que la conexión ha sido establecida con el PLC a través de una identificación de logueo por inicio de sesión única (Single Sign-On, SSO[73], por sus siglas en inglés), con credenciales de administrador del dispositivo. Por este motivo se puede acceder a apagar, arrancar y localizar físicamente el PLC (parte inferior derecha de la Figura 48).

Para la programación de los PLC es necesario el uso de los medios que ofrece el software de ingeniería TIA Portal. Éste otorga la capacidad de programar los sistemas de diferentes maneras, acorde a los principales lenguajes de programación existentes como son:

[72] Esta estructura algebraica se corresponde con la esquematización de las operaciones lógicas aplicadas en el campo de la electrónica digital, la informática y las matemáticas.

[73] El inicio de sesión único, se corresponde con un procedimiento de autenticación, que permite al usuario acceder a varios sistemas con una sola instancia de identificación.

- ***FUP.*** Es un lenguaje de Step7 gráfico que utiliza los cuadros del álgebra booleana para representar la lógica. Asimismo, permite representar funciones complejas (p.ej. funciones matemáticas) mediante cuadros lógicos. Tiene la ventaja de proporcionar la visión agrupada por bloques de las diferentes lógicas, disponiendo a su vez de bloques complejos. Cuando existe una cantidad amplia de elementos correspondientes a la lógica booleana en serie, suele ser más compacto y fácil de ver el segmento completo.
- ***KOP.*** Se corresponde con un esquema de contactos, escalera o "ladder". Es un lenguaje de Step 7 gráfico y posiblemente el más extendido en todos los lenguajes de programación, y por tanto el más similar a otros. Probablemente es el más fácil de entender por personal proveniente de la industria eléctrica y técnicos eléctricos. En definitiva, es la representación que habría que materializar y cablear si se quisiera hacer el mismo programa que se realiza con el PLC.
- ***AWL.*** Es un lenguaje de programación textual orientado a la máquina. En un programa creado en AWL, las instrucciones equivalen en gran medida a los pasos con los que la CPU ejecuta el programa. Para facilitar la programación, AWL se ha ampliado con estructuras de lenguajes de alto nivel (tales como accesos estructurados a datos y parámetros de bloques). Es el más completo y el más complejo visualmente de seguir. Para instrucciones sencillas es muy útil pero cuando se quiere hacer una lógica un poco compleja el trabajo de seguimiento y de depuración es complicado y fácilmente susceptible de cometer errores. Por otra parte los lenguajes FUP y KOP gráficos son traducibles a AWL, pero no al revés y no necesariamente entre ellos.

Concretamente SIEMENS, a través de TIA Portal, ha desarrollado un lenguaje de alto nivel estructurado denominado SCL.

Este lenguaje se corresponde con la norma IEC 6113-3 (ST) [Xiong J., 2021], el cual facilita la integración de código en los procesos de codificación.

Referente a los lenguajes de programación usados, hay que destacar que la unidad central de proceso del PLC S7 1200, organiza de manera interna, los bloques de programación, distribuyendo las diferentes funcionalidades permitidas por el software de ingeniería, diseñados y programados éstos mediante TIA Portal. La ventaja principal de esta arquitectura se corresponde con la eficiencia de la estructuración de las funciones, programas, etc. del programa realizado.

Estos bloques lógicos se corresponden con:

- *Los bloques de organización* (Organization Block, OB, por sus siglas en inglés) definen la estructura del programa. Algunos OB tienen reacciones y eventos de arranque predefinidos. No obstante, también es posible crear OB con eventos de arranque personalizados. En el caso que nos ocupa, se ha diseñado el programa de gestión de los semáforos de tráfico, estando éste ubicado en el OB.

  Las Figuras 55 a la 60, se corresponden con la programación específica llevada a cabo para la investigación ejecutada con la CAI-1. Los diversos segmentos están asociados con las diferentes etapas programadas y en sus diferentes estados.

- *Las funciones* (Functions, FC, por sus siglas en inglés) y los bloques de función (Functions Blocks, FB, por sus siglas en inglés) contienen el código de programa correspondiente a tareas específicas o combinaciones de parámetros. Cada FC o FB provee parámetros de entrada y salida para compartir datos con el bloque que ha invocado la llamada. Un FB también utiliza un bloque de datos asociado DB de instancia (Data Block, DB por sus siglas en inglés) para conservar los valores de datos para la instancia de la llamada de FB.

- *Los bloques de datos* (Data Bases, DB, por sus siglas en inglés) almacenan datos que pueden ser utilizados por los bloques del programa.

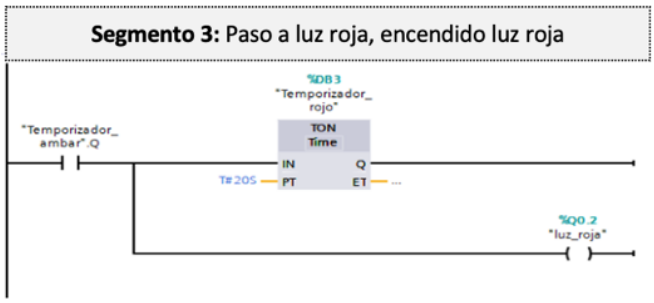


Figura 55: Segmento programación (proceso de encendido de la luz roja).

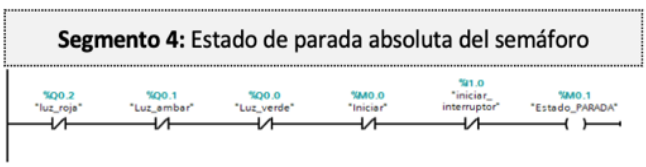


Figura 56: Segmento programación (proceso de parada del semáforo).

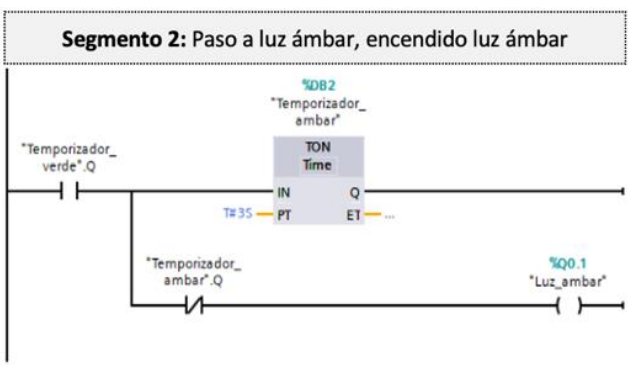


Figura 57: Segmento programación (proceso de encendido de la luz ámbar).

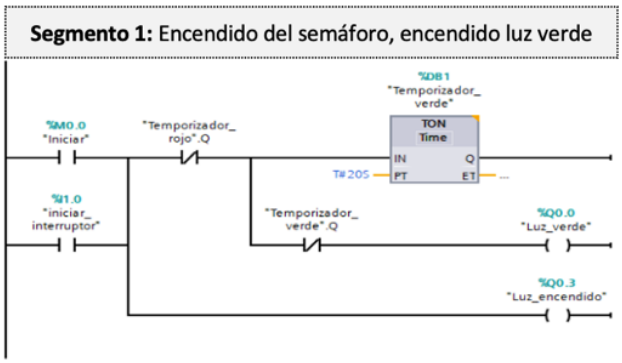


Figura 58: Segmento programación (proceso de encendido de la luz verde).

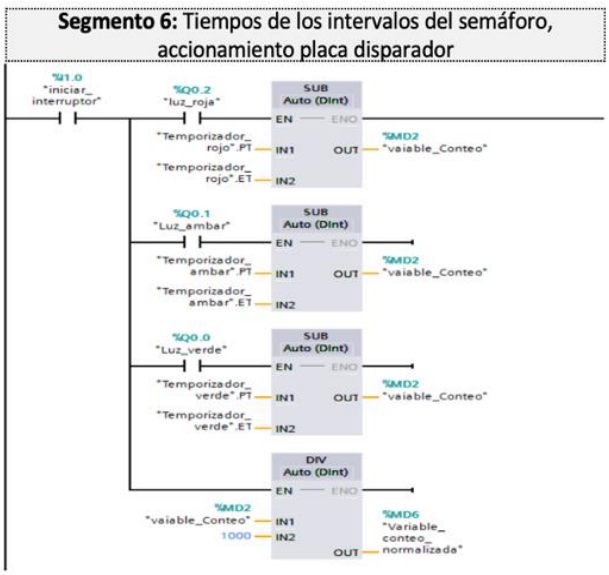


Figura 59: Segmento programación (programación de tiempos intervalos a través de la placa disparadora).

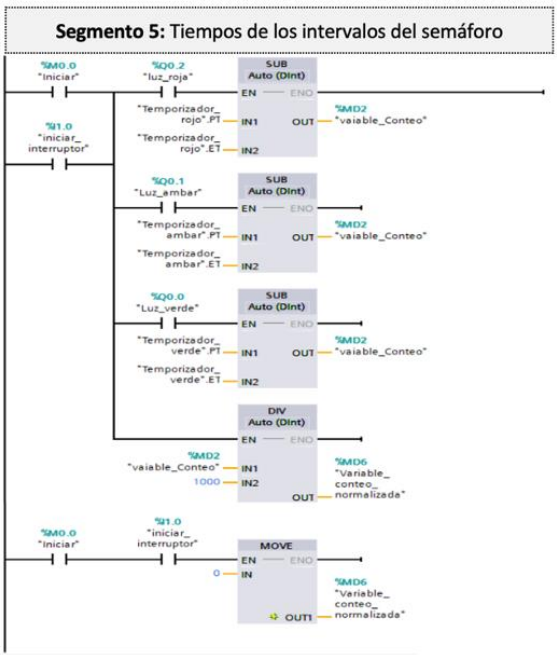


Figura 60: Segmento programación (programación de tiempos de intervalos del semáforo).

Una función (FC) o un bloque de función (FB) es un bloque de código del programa que puede ser invocado desde un OB, o bien desde otra FC u otro FB. El nivel de anidamiento de invocaciones permitido por este modelo de PLC es dieciséis desde OB de ciclo o de arranque y seis desde cualquier OB de evento de alarma, por lo que cubre con creces las necesidades planteadas en la investigación trazada.

Otros de los motivos que influyeron para la elección de este modelo concreto de PLC (ver Figura 61) fue la capacidad para la ejecución del programa necesario para cada evaluación de entorno. Es un dispositivo con amplias capacidades en su memoria de carga[74] disponible y la memoria de

[74] La memoria de carga esta memoria difiere dependiendo de la CPU del PLC (1211,1212 y 1214) permite almacenar de forma no volátil el programa de usuario, los datos y la configuración. El programa de usuario es alojado en primera instancia en este área de la CPU.

trabajo de la CPU. La limitación total del número de bloques en ejecución que es capaz de manejar este modelo de PLC se limita a 1024.

Figura 62: Placa identificativa del PLC S7 1200

Figura 61: Placa de interruptores (entradas digitales).

Otra de las características que posee este PLC, y que ha servido para poner en práctica ciertos aspectos de la investigación desarrollada, es su capacidad de despliegue de un servidor web. El servidor web para el S7-1200 ofrece:

1. Acceso mediante página web a datos de la CPU y de proceso desde un PC o un dispositivo móvil.
2. Muestra las páginas en un formato y tamaño compatibles con el dispositivo que utiliza para acceder a las páginas web.
3. El servidor web admite una resolución mínima de 240 x 240 píxeles.
4. Para acceder a su pantalla de configuración, mediante la conexión a través de la dirección IP de la CPU S7-1200, ésta se establece mediante el uso de un navegador web y una conexión de red establecida mediante conector RJ45 con el PLC.
5. El S7-1200 soporta varias conexiones concurrentes. Para alcanzar un área más amplia correspondiente a los modelos de interactuación ante la evaluación de ciertas vulnerabilidades a testear en SICERCAI, como se puede apreciar en la imagen correspondiente a cada uno de los PLC (Figura 53) se han incorporado dos módulos de simulación de SIEMENS

para usar en las entradas digitales del cada PLC SIMATIC S7 1200 (ver Figura 62). Estos módulos permiten la generación de eventos directamente sobre el programador, facilitando interactuar ante un escenario de prueba mediante la materialización de un posible ataque físico-cibernético.

Cada PLC cuenta con una placa identificativa que refleja las principales características técnicas del controlador. En la Figura 61 se muestra la placa correspondiente a los PLC incorporados en la CAI-1. Para la consulta del manual técnico completo de este modelo de instrumentación industrial, puede consultarse el repositorio creado al efecto [URL- 00, 2021].

4.8.2. SCALANCE S615

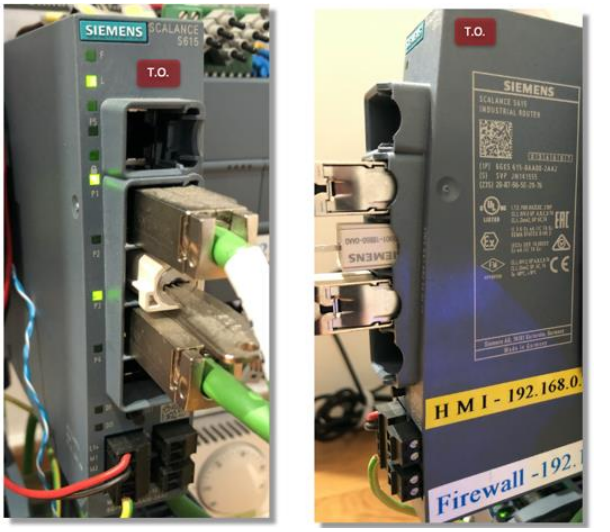


Figura 63: SCALANCE S615, instalado en la CAI-1.

Como se puede apreciar en la Figura 63 se ha incorporado un cortafuego industrial de la familia SCALANCE, modelo S615 en la CAI-1. Los módulos de seguridad de la familia SCALANCE S disponen de una fácil conexión y adaptabilidad para ser incorporados al mundo CTITO. Están especialmente diseñados para satisfacer las exigencias de los sistemas de

automatización con características tales como un diseño resistente para entornos industriales, fácil instalación y un mínimo tiempo de inactividad.

Es destacable que el módulo de seguridad SCALANCE S615 cuenta con cinco puertos Ethernet que ofrecen protección para varias topologías de red a través de un cortafuegos o una red privada virtual (Virtual Private Network, VPN por sus siglas en inglés) (IPsec y OpenVPN), permitiendo una implementación flexible de las diferentes conexiones a los entornos de pruebas de manera segura.

A su vez, ofrece la posibilidad de configurar hasta cuatro zonas de seguridad variables con reglas de cortafuegos individuales, lo que ofrece versatilidad para interconectar varias CAI usando un solo firewall.

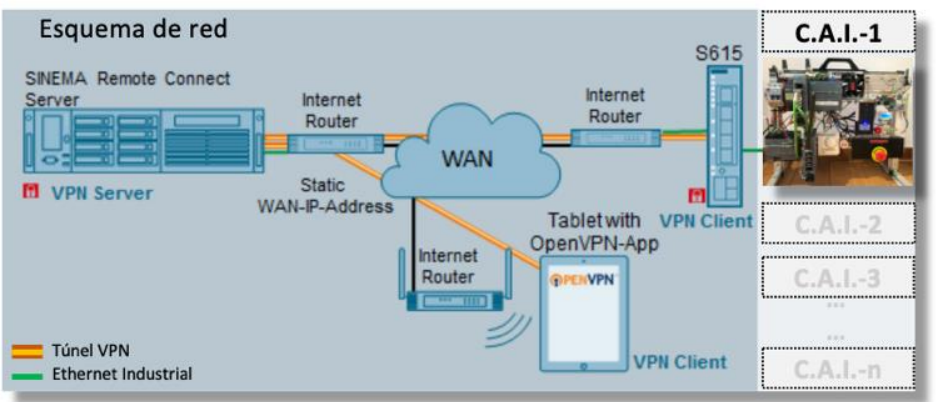


Figura 64: Esquema de conexión de red entre el tunelador VPN (SRC) y el Scalance S615.

La Figura 64 detalla de manera gráfica un ejemplo de arquitectura de red de acceso remoto a las TO en la que se encuentra desplegado un SRC, el cual establece una línea de datos segura a través de VPN con el firewall industrial de la serie S615.

Gracias a la interfaz de autoconfiguración, el dispositivo puede integrarse y parametrizarse fácilmente con la plataforma de gestión del conector remoto (Sinema Remote Connect, SRC por sus siglas en inglés). Como se puede apreciar en la Figura 65, en el S615 está habilitada la conexión contra un SRC en el firewall desplegado en SICERCAI,

encontrándose habilitada la conexión al SRC para establecer y crear un túnel VPN en las comunicaciones entre usuarios demandantes del sistema de pruebas el acceso remoto.

El modelo establecido y desplegado en SICERCAI cumple con las guías de buenas prácticas y recomendaciones de seguridad en lo que a arquitectura de redes industriales y operacionales del fabricante se refiere

El SCALANCE S615 permite la creación de varias redes virtuales de área local (Virtual Local Area Network, VLAN, por sus siglas en inglés) para que, de acuerdo con los permisos concedidos a las diferentes máquinas virtuales, se conceda el acceso bidireccional entre los PLC a la HMI, los PLC al sistema de programación con TIA Portal y los PLC al SCADA.

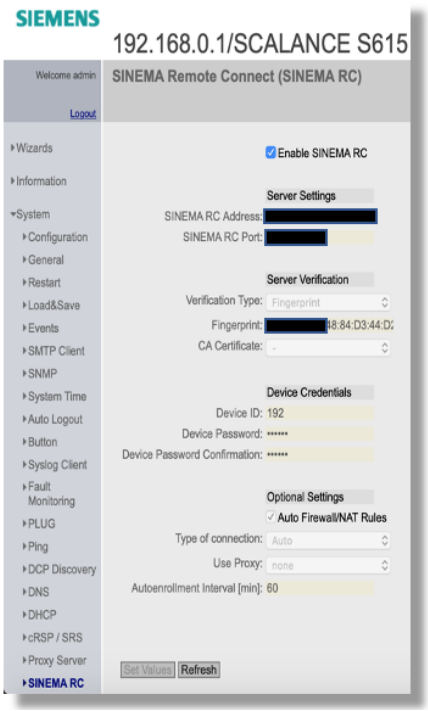


Figura 65: Pantalla de configuración del SCALANCE S615 con conexión a SRC habilitada.

El nuevo módulo de seguridad SCALANCE S615 tiene opciones diferentes de configuración, gestión y diagnóstico a través de la gestión basada en la web (Web Based Management, WBM por sus siglas en inglés),

interfaz de línea de comandos (Command Line Interface, CLI por sus siglas en inglés) y el protocolo de gestión de red simple (Simple Network Management Protocol, SNMP, por sus siglas en inglés). Como un servidor de protocolo de configuración dinámica de host (Dynamic Host Configuration Protocol, DHCP, por sus siglas en inglés) y el cliente, el dispositivo puede ser utilizado en cualquier red de área local (Virtual LAN, VLAN, por su acrónimo en inglés, zona de seguridad virtual). El nuevo dispositivo tiene una función de interruptor de llave en su entrada digital para establecer una conexión de túnel controlado.

Dependiendo del nivel de seguridad requerido para cada conexión a establecer, las características de seguridad de firewall y VPN pueden ser configuradas individualmente.

En la Figura 66, se pueden observar, una de las pantallas de configuración que ofrece este dispositivo.

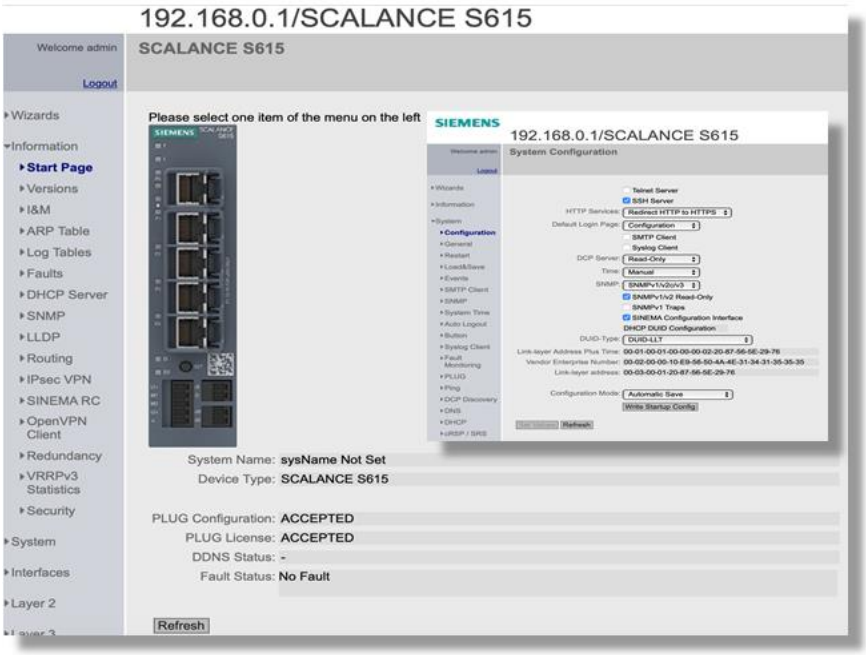


Figura 66: Página principal de configuración del SCALANCE S615.

El SCALANCE S615 cuenta con una placa identificativa que refleja las principales características técnicas inherentes al dispositivo.

La Figura 67 muestra la placa correspondiente al S615 incorporado en la CAI-1. Para la consulta de toda la información técnica al completo de este modelo de instrumentación industrial, puede consultarse el repositorio creado al efecto [URL- 00, 2021].

Figura 67: Placa identificativa del SCALANCE S615.

4.8.3. Sinema Remote Connect

El SRC se corresponde con una plataforma de gestión, creada y suministrada por SIEMENS, para garantizar un acceso remoto, eficiente y seguro a las células de automatización industrial y a los laboratorios de pruebas y maquetas industriales que se establezcan. La aplicación se basa en conexiones cliente-servidor (véase la Figura 68).

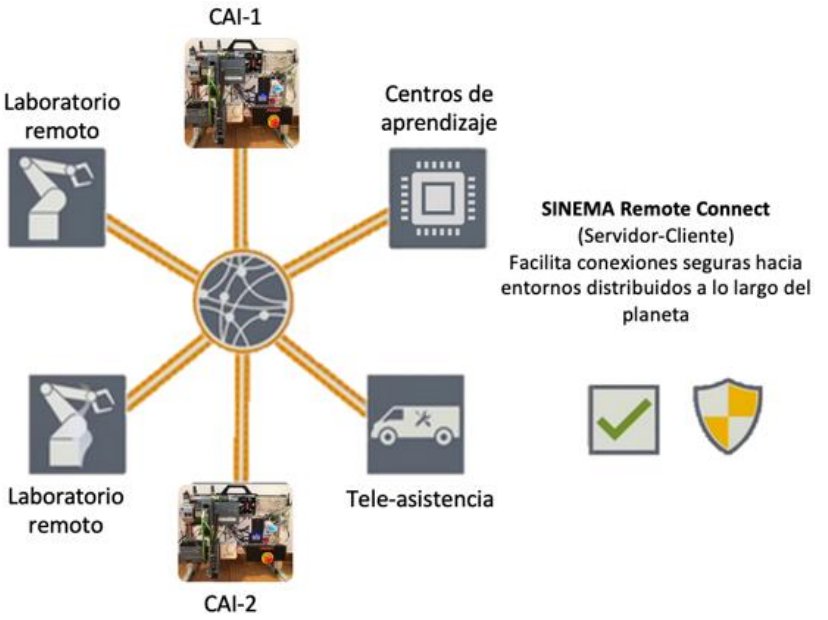


Figura 68: Esquematización representativa de la conectividad a través de SRC (Conexiones tipo cliente-servidor).

En SRC la aplicación del lado del servidor simplifica no sólo servicios remotos, como el mantenimiento a distancia de las máquinas y plantas, sino también otras aplicaciones remotas, como la monitorización de las condiciones de acceso. SRC gestiona y autoriza a todos los enlaces de comunicación. La plataforma de gestión es particularmente adecuada para la gestión de las comunicaciones y accesos a la CAI, ya que permite a los usuarios de los equipos el control de cada uno de los componentes accesibles a través del SCALANCE S615.

El SRC garantiza la administración segura de túneles VPN entre el centro de control, las estaciones de ingeniería y usuarios de éstas (TIA Portal)

y las CAI instaladas. Su forma de gestionar las conexiones es mediante la verificación de la identidad de las CAI que se incorporen a SICERCAI individualmente mediante el intercambio de certificados, previamente a la concesión de cualquier acceso a la máquina.

Cualquier acceso no autorizado a las redes asociadas a SICERCAI en las que las diferentes células operan es bloqueado aumentando así la seguridad. Las conexiones a través del túnel VPN se realizan en conformidad con la norma OpenVPN basada en certificados protegidos mediante cifrado de hasta 4096 bits [Gómez L., 2018].

Otra de la las ventajas que posicionaron al SRC para ser desplegado en SICERCAI fue la capacidad de asignación de derechos de acceso a las máquinas. Esas capacidades pueden ser reguladas de manera central utilizando la función de administración de usuario simple de la plataforma de gestión. Todas las CAI que se desplieguen pueden ser habilitadas o bloqueadas de forma manual, por lo que los usuarios del laboratorio de pruebas y operadores de las CAI también tienen un control permanente sobre todos los intentos de acceso a su red de operación. Todas las CAI pueden ser identificadas y seleccionadas a través del SRC. Las conexiones VPN se establecen de una manera sencilla. SRC posee la cualidad de ser independiente del protocolo que en los elementos industriales se hayan desplegado. Esto significa que los usuarios pueden utilizar diferentes aplicaciones, tales como el software de programación STEP 7 Simatic (TIA Portal) para mantenimiento remoto tan pronto como se haya establecido la conexión a la máquina.

Otro de los grandes beneficios que ofrece para el sistema de conocimiento por experimentación real creado es que las diferentes células de automatización industrial que formen parte de SICERCAI pueden ser

conectadas a SRC a través de redes de telefonía móvil, ADSL o infraestructuras de redes privadas existentes.

SIEMENS ofrece una amplia cartera de rúters industriales de la serie SCALANCE adecuados para este propósito. En el seno de esta investigación se han incorporado el SCALANCE S615, el M876-4 y el W778-1. Estos dispositivos pueden ser fácilmente parametrizables a través del SRC, usando una interfaz de configuración automática. Toda la información sobre las respectivas máquinas puede ser almacenada en la plataforma de gestión, lo que significa que los rúters sólo tienen que registrarse una vez en SRC, después de lo cual todos los datos de configuración son asignados a ellos.

La Figura 69 esboza una posible configuración general correspondiente al despliegue de un SRC para la protección de los accesos a las diferentes CAI en SICERCAI.

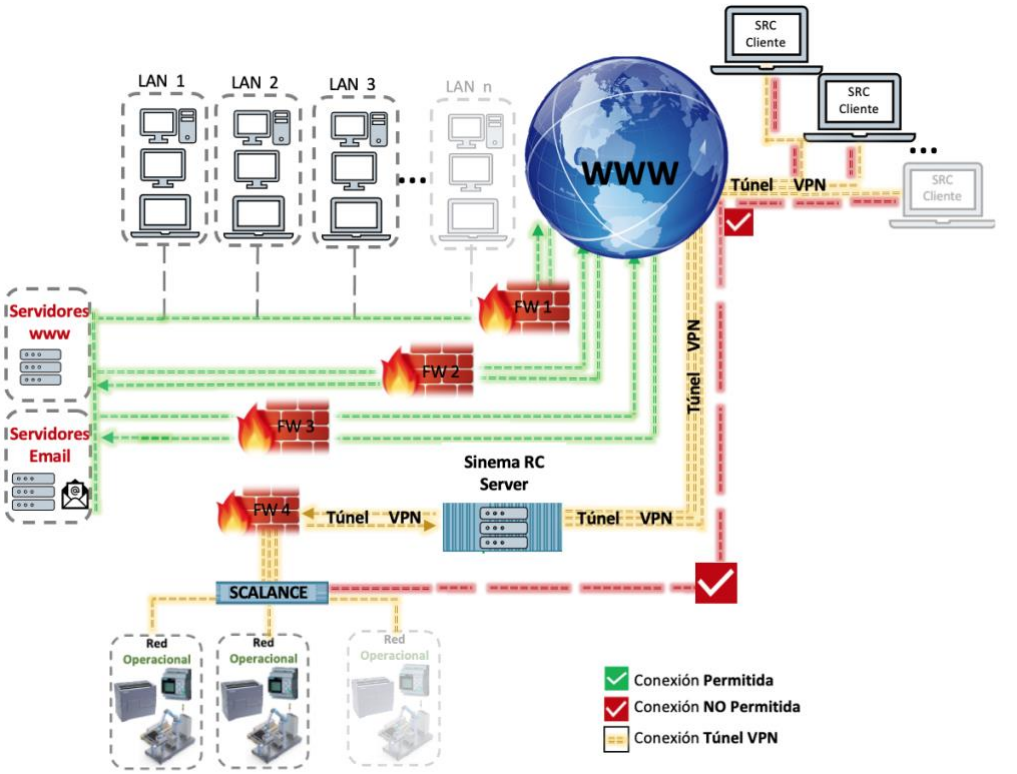


Figura 69: Descripción de una arquitectura de red con un SRC desplegado para conexiones a través de VPN a redes operacionales.

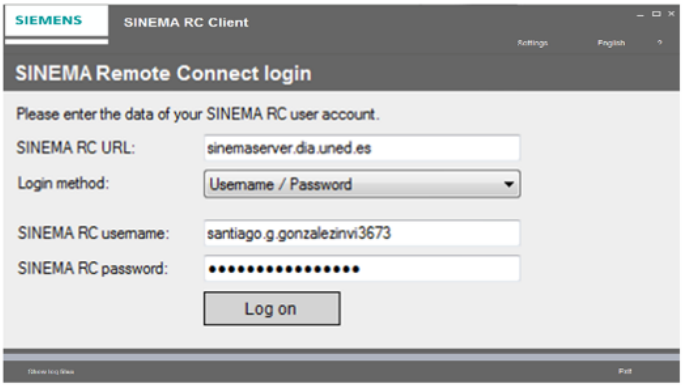


Figura 70: Pantalla de identificación de SRC tras el establecimiento de la conexión.

La Figura 70 se corresponde con la ventana emergente suministrada por el cliente del Sinema RC al realizarse el establecimiento de una conexión hacia el servidor de SRC. En la Figura 64 se ha detallado la conexión entre el servidor y los clientes del tunelador VPN.

4.8.4. SCALANCE W778-1 (SIMATIC NET IWLAN Access Point)

Figura 71: Imagen correspondiente al SCALANCE W778-1 incorporado en la CAI-1.

El SCALANCE W778-1 (Figura 71), utilizado en la célula de automatización industrial CAI-1, se corresponde con un punto de acceso inalámbrico de diseño compacto y robusto que ha permitido su

incorporación al proyecto de un modo sencillo. Esta adhesión proporciona un valor extra a SICERCAI puesto que un punto de acceso inalámbrico a una infraestructura de las TO representa de manera práctica el sustento y aprovechamiento de las TI y las TO en el área operacional, y con la consiguiente exposición a las nuevas vulnerabilidades y riesgos asociados a este tipo de arquitecturas.

Figura 72: Página principal de configuración del SCALANCE W778-1

Este punto de acceso no difiere en absoluto de los existentes en TI en lo que se refiere a la conectividad. La transmisión de datos la materializa conforme al estándar WLAN IEEE 802.11n [URL- 104, 2021], [URL- 105, 2021] admitiendo bandas de frecuencias de 2,4 y 5 gigahercios (GHz). A su vez este dispositivo puede ser integrado con TIA Portal (disponible en la máquina virtual de simulación de la estación de ingeniería), siendo idóneo para la recreación de un acceso inalámbrico, el cual puede ser susceptible de asumir un rol de vector de ataque hacia una infraestructura de TO, viniendo a resaltar todo aquello explicado y detallado sobre las problemáticas asociadas a la interconexión de los mundos de las TI y de las TO.

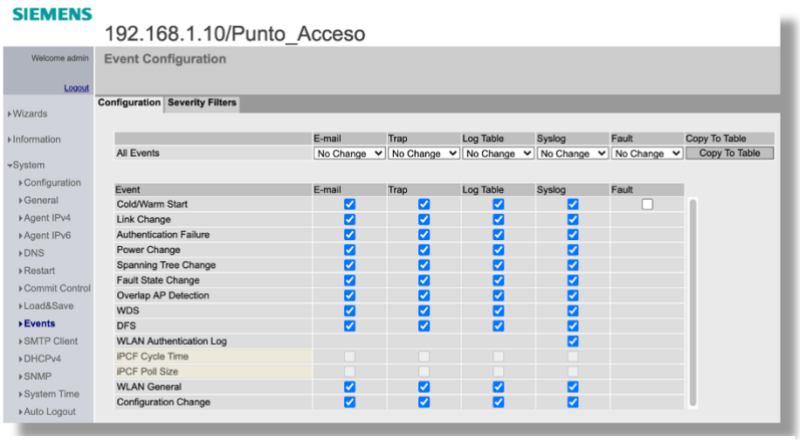


Figura 73: Página principal de configuración del SCALANCE W778-1

Al igual que los dispositivos detallados con anterioridad, el SCALANCE W778-1 dispone de un servidor web al que se puede acceder de modo remoto, permitiendo una configuración personalizada a través de los numerosos parámetros de configuración disponibles. En la Figura 72, se muestra una captura de pantalla del servidor web que da acceso al dispositivo tras haberse identificado debidamente.

Pantalla de configuración de eventos del SCALANCE W778-1.

Las Figuras 73 y 74 obtenidas directamente del SCALANCE W778-1, se corresponden con las opciones de configuración del DHCP y el menú de configuración de los eventos registrados por el punto de acceso, respectivamente. Estas configuraciones reflejan la disposición específica creada para SICERCAI en lo referente a la configuración dinámica del host (DHCP).

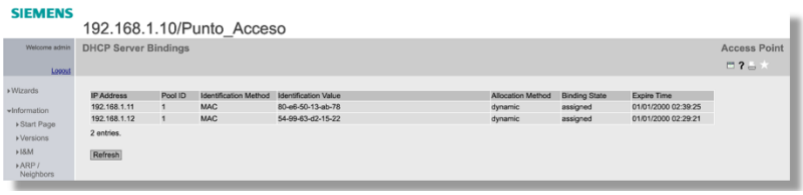


Figura 74: Configuración del DHCP en SICERCAI.

La configuración del registro de eventos es de suma importancia por su aporte de información a la hora de poder ser analizado tras registrar

cualquier acontecimiento. Estas capacidades se ven potenciadas ante eventos susceptibles de causar disrupciones en materia de ciberseguridad.

En la Figura 75, se muestra la placa identificativa del producto correspondiente al SIMATIC NET, IWLAN W778-1 incorporado en la CAI-1. Para la consulta de toda la información técnica al completo de este modelo de instrumentación industrial, consúltese el repositorio creado al efecto [URL- 00, 2021].

Figura 75: Placa identificativa del SCALANCE W778-1.

4.8.5. Instrumentación incorporada ajena al ámbito industrial

Una vez detallados los dispositivos correspondientes a la instrumentación operacional que se han incorporado en la CAI-1 para completar y otorgar ciertas capacidades extras a modo laboratorio de pruebas de elementos de las TI, se han añadido los elementos mostrados en la Figura 70. La instrumentación que se especifica se encuentra debidamente cableada a las entradas digitales de los PLC.

La justificación de este acoplamiento es proporcionar las capacidades de entrenamiento e interactuación con los controladores programables sin necesidad de ser acoplados a entornos de pruebas más complejos.

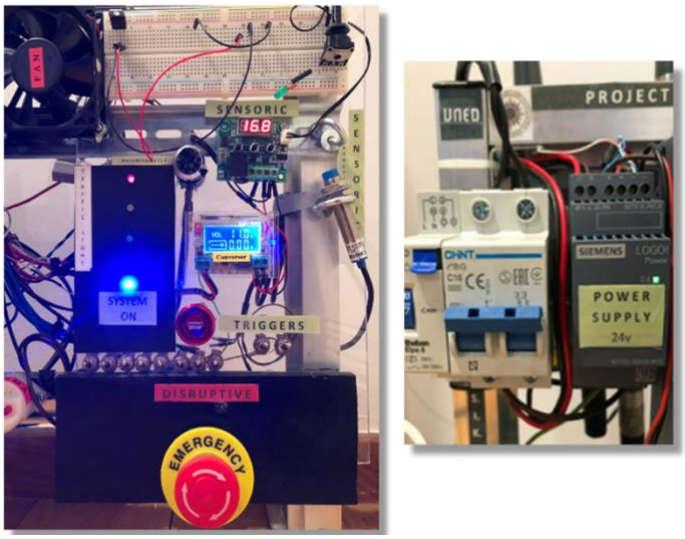


Figura 76: Componentes IT en la CAI-1 así como fuente de alimentación de 24v.

Por esta situación, SICERCAI cumple con varias premisas establecidas para su desarrollo, ostentando la capacidad de poseer una alta cohesión con otros sistemas, portabilidad, escalabilidad y capacidad de análisis.

Correspondiente a las Figuras 77 (a), (b), (c), (d) y (e), se detallan los componentes de las TI incorporados a la CAI-1.

(a) *(b)* *(c)* *(d)* *(e)*

Figura 77: Componentes TI incorporados en la CAI-1.

- ***Figura 71-(a).*** Corresponde a una sonda digital de registro de temperatura. Este tipo de sensor ayuda a ejecutar pruebas de control PID.
- ***Figura 71-(b).*** Representa un conversor de voltaje y amperaje. Esto es importante ya que existen sensores que necesitan un suministro energético diferente al proporcionado por la fuente de alimentación incorporada para la instrumentación industrial (ver Figura 76).
- ***Figura 71-(c).*** Se corresponde con los disparadores y un pulsador de emergencia de corte de alimentación al PLC 2 de la CAI.

- ***Figura 71-(d).*** Un termostato analógico el cual proporciona otro rango de medición. Estas medidas pueden ser asociadas al programa cargado en el PLC para el registro de las acciones especificadas el bloque principal del controlador lógico programable.
- ***Figura 71-(e).*** Sensores inductivos. Este elemento está diseñado para la detección de elementos ferrosos, dando cabida a la simulación de multitud de escenarios en entornos TO.

4.8.6. HMI (Human Machine Interface)

Figura 78: Diferentes HMI del fabricante SIEMENS.

Viniendo a completar el entorno desplegado en SICERCAI para la recreación de un sistema de control industrial completamente adecuado a la realidad operacional, y cuya misión es realizar el control remoto de las acciones implementadas en el autómata programable de la CAI-1, se ha creado una interface hombre-máquina (Human Machine Interface, HMI por sus siglas en inglés) a través de un panel táctil simulado. Todo ello ha sido desarrollado a través del TIA Portal. Estos paneles (Figura 78) ofrecen la interfaz adecuada para cada aplicación programada en los autómatas y el campo de TO. Concretamente, la serie básica de estas pantallas (series SIMATIC HMI, Comfort Panels) [URL-106, 2021], ofrecen las cualidades necesarias y suficientes para su conexión a los PLC de la célula de automatización industrial, y, por consiguiente, la gestión y el control del

sistema de control de tráfico implementado. Son programados mediante el software de ingeniería TIA Portal existente en la máquina virtual de soporte y programación de ingeniería.

(a) *(b)* *(c)*

Figura 79: Pantallas principales del HMI correspondiente a los diferentes menús creados para el proyecto.

En la Figura 79 (a) se puede apreciar la administración de usuarios o el acceso al núcleo del sistema de gestión industrial. Tras la adecuada verificación de las credenciales en la pantalla anteriormente mostrada, se pueden ver las posibilidades de administración de los procesos creados en el CAI-1 (Figura 79 (b)). Esta imagen muestra la posibilidad de gestionar los derechos de los diferentes tipos de usuarios que pueden interactuar con el IAC 1. Este panel de gestión de usuarios (Figura 79 (c)) es de vital importancia desde el punto de vista de la ciberseguridad de los sistemas, ya que se puede acceder al núcleo de la funcionalidad industrial de forma remota otorgando para ellos los debidos permisos a los grupos de usuarios.

El panel de control remoto dispone de varias pantallas de navegación que ofrecen diferentes posibilidades de gestión. La Figura 80 muestra las imágenes de los sistemas de control a los que a través del puerto de comunicación RJ45 son accesibles y se encuentran simulados como conexión física al HMI afiliado al proyecto.

(a) *(b)* *(c)*

Figura 80: Sistemas de control simulados a través de HMI y TIA Portal.

En orden de izquierda a derecha, éstas se corresponden con un controlador PID, un controlador gráfico del tiempo de cambio entre luces de los semáforos y una maqueta de cuatro tanques para la gestión de procesos simulados en el sector químico.

Al mismo tiempo se ha implementado un controlador PID para el control de gestión de los procesos; puede ser ajustado manual y automáticamente con parámetros predefinidos (Figura 80 (a)). A su vez, según se observa en la Figura 80 (b), para poder realizar un control analítico de patrones de señales originadas por los cambios necesarios en cualquier sistema de control de tráfico, se ha optado por la creación de un modelado gráfico de las señales. Así mismo, la Figura 80 (c) representa un sistema, bajo un control táctil y remoto, de la maqueta de 4 tanques física, ubicada en el laboratorio del departamento de Informática y Automática de la UNED.

Las Figuras 81 (a), (b) y (c), muestran los estados y correspondencias de luces en el HMI de control de tráfico, creado para la investigación presentada en este capítulo.

(a) *(b)* *(c)*

Figura 81: Pantallas del HMI, sistema control de tráfico.

La incorporación de esta pantalla de interfaz hombre-máquina en SICERCAI, virtualizada y programada mediante el software de ingeniería TIA Portal, ha sido estrictamente necesaria para poder llevar a su debida ejecución las pruebas de concepto bajo un entorno controlado de una disrupción funcional de un sistema. En concreto la alteración del sistema de control de tráfico automovilístico y peatonal.

Se puede consultar toda la información técnica al completo de este modelo de instrumentación industrial así como sus cualidades físicas, en el repositorio creado al efecto [URL- 00, 2021].

4.9. Desarrollo (TIA Portal Ingeniería, tareas implementadas)

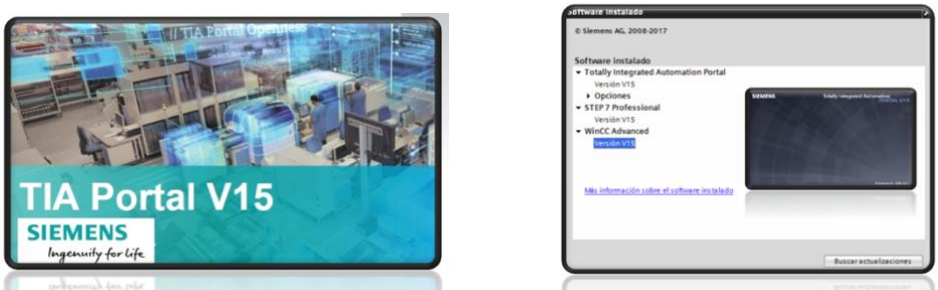


Figura 82: Software de ingeniería TIA Portal

Tras haber detallado toda la instrumentación industrial que forma parte de la célula de automatización industrial CAI-1 en SICERCAI, es necesario disponer del software concreto que facilite la programación de las

distintas funcionalidades de esos dispositivos de las TO. Para esta labor se ha utilizado el software propietario de SIEMENS TIA Portal, en sus versiones 15 y 15.1, así como STEP 7 Professional y WinCC Advance para el diseño y configuración del HMI (Figura 82).

El software TIA Portal es un innovador sistema de programación de ingeniería que permite una configuración intuitiva y eficiente de todos los procesos de planificación y producción, así como una reducción de costes en mantenimiento y despliegue.

SIEMENS, en una publicación de los estudios llevados a cabo relativos a la eficiencia que ofrece TIA Portal, corrobora que el software de ingeniería *"incrementa la disponibilidad de las aplicaciones en planta de producción obteniendo de hasta un 99% de incremento de la disponibilidad, y al mismo tiempo supone un ahorro en los costes de mantenimiento de hasta un 15%"* [SIEMENS, 2014].

La principal utilidad que TIA Portal proporciona es la posibilidad de constituir distintas aplicaciones de software industrial para procesos de producción a través de un mismo interfaz de una manera integral y automática. Ofrece un entorno de ingeniería unificado para todas las tareas de control, visualización y gestión. Esta acción provee grandes capacidades para el aprendizaje, la interconexión y la operación, pilares básicos sobre los que se sustenta el propósito de la investigación de esta Tesis. No importa si se trata de la programación de un controlador (PLC S7 200, 300, 1200, etc.), de la configuración de una pantalla HMI (Confort Panel Basic, WinCC, etc.) o de la parametrización de los accionamientos: con este tipo de software tanto los usuarios noveles como los expertos programadores industriales pueden desarrollar entornos de ingeniería de las OT, de manera instintiva, efectiva y eficiente ya que no precisan operar sobre una amplia diversidad de sistemas y herramientas procedentes de diferentes áreas industriales. Otra gran

ventaja que ofrece es que se trata de una aplicación modular a la que se le pueden ir añadiendo nuevas funcionalidades según las necesidades concretas de cada sector industrial en las que sean necesario desplegar un entorno a evaluar dentro de SICERCAI.

De igual manera otro punto a destacar del uso de este sistema de programación modular, recae sobre el coste económico de la inversión a realizar en sistemas de programación en ingeniería, viniendo a abaratar esta necesidad.

Esta integración en una sola plataforma (Totally Integrated Automation Portal, Portal De Integración Totalmente Integrado), según un estudio llevado a cabo por SIEMENS [URL- 107, 2021], facilita la obtención de una tasa de ahorro en los elementos del software industrial a lo largo de su ciclo útil de vida de producción de hasta un 30%, motivo más que suficiente para ser justificable su adhesión a SICERCAI.

El TIA Portal incorpora las últimas versiones del software de ingeniería SIMATIC STEP 7, WinCC y Start-Drive para la planificación, programación y diagnóstico de todos los controladores SIMATIC, las pantallas de visualización y la última generación de accionamientos SINAMICS.

Los lenguajes de programación soportados por la plataforma TIA Portal, y con los que se han diseñado las funcionalidades de la CAI-1 con componentes SIEMENS, han sido descritos con anterioridad. Los dos proyectos programados con TIA para la sustentación de los pruebas de concepto se corresponden con los sub-apartados que se describen a continuación. A través de ellos se describen los árboles de proyectos respectivos, las variables implementadas necesarias para su recreación y las herramientas tecnológicas programadas para su control de cada uno de los proyectos.

- ***SICERCAI -1.*** *Proyecto de regulación y control de luces de tráfico de vehículos y peatones.* Las Figuras 83, 84 y 85 y 86, representan gráficamente su contenido.

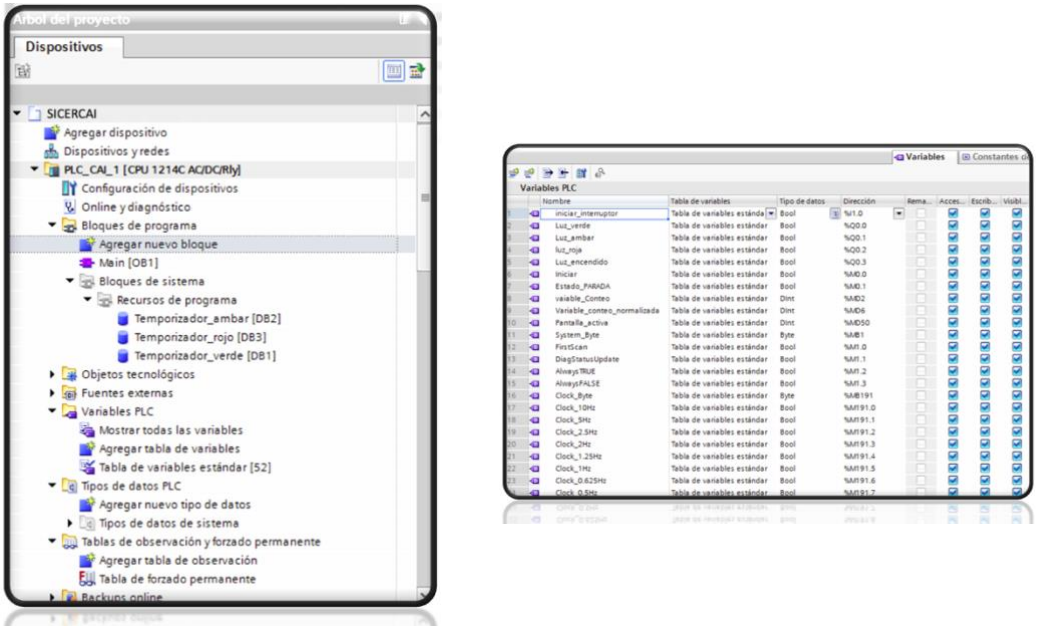


Figura 85: Imagen correspondientes al árbol del proyecto SICERCAI-1 y variables declaradas (TIA Portal).

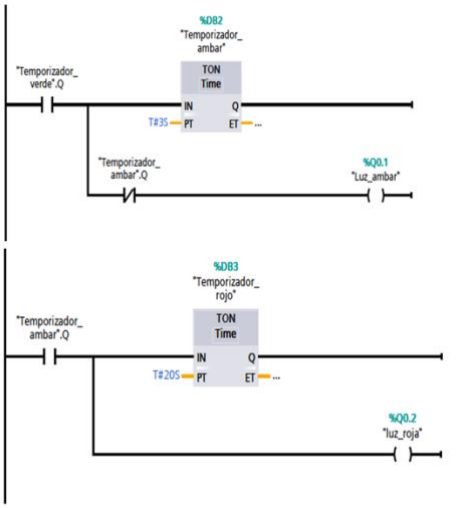


Figura 84: Contenido MAIN [OB1] del proyecto SICERCAI-1 segmentos 3, y 4.

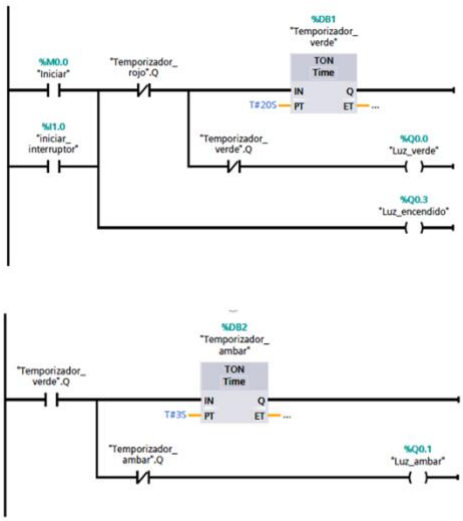


Figura 83: Contenido MAIN [OB1] del proyecto SICERCAI-1, SEGMENTOS 1 y 2.

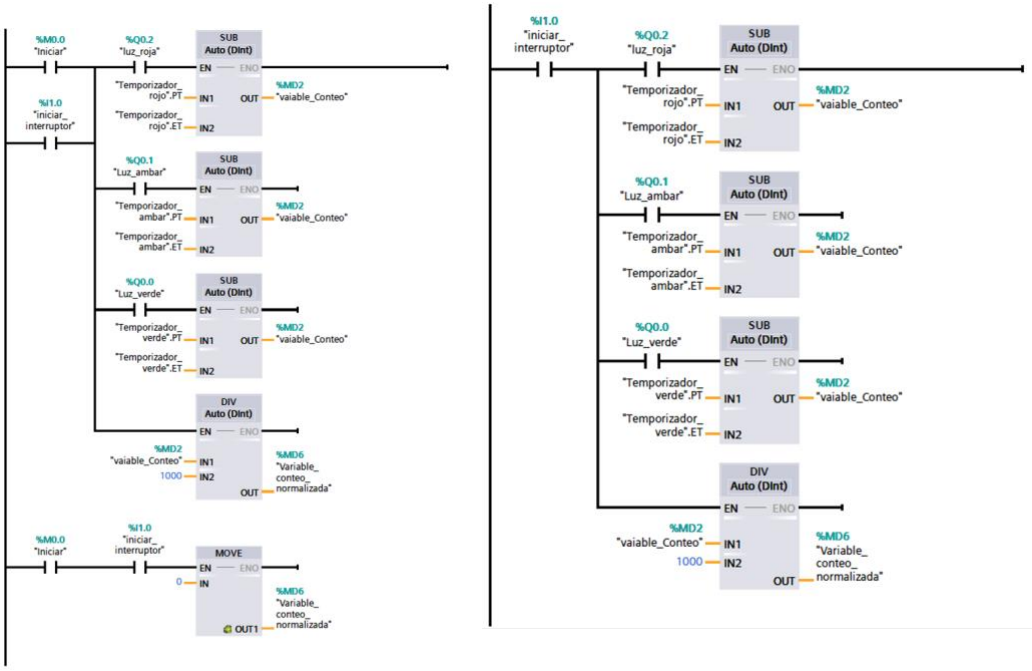


Figura 86: Contenido MAIN [OB1] del proyecto SICERCAI-1 segmentos 5 y 6.

La Figura 83 muestra la representación gráfica, que se corresponde con el árbol de directorios que ofrece el software de ingeniaría TIA Portal, en función del hardware que se esté utilizando para su programación (PLC, HMI, SCALANCE, etc.). Concretamente se muestran todos aquellos intervinientes en el proyecto denominado SICERCAI, y el PLC-CAI_1 (Célula de Automatización Industrial 1).

- ***SICERCAI -2****. Proyecto de regulación, control y gestión de procesos a través de una maqueta industrial de cuatro tanques.* Las Figuras 87, 88 y 89 representan gráficamente el contenido del proyecto a través de TIA Portal. Representa concretamente los elementos necesarios para la programación de un segundo PLC 1214_ACDC_Relay, incorporado al proyecto SICERCAI.

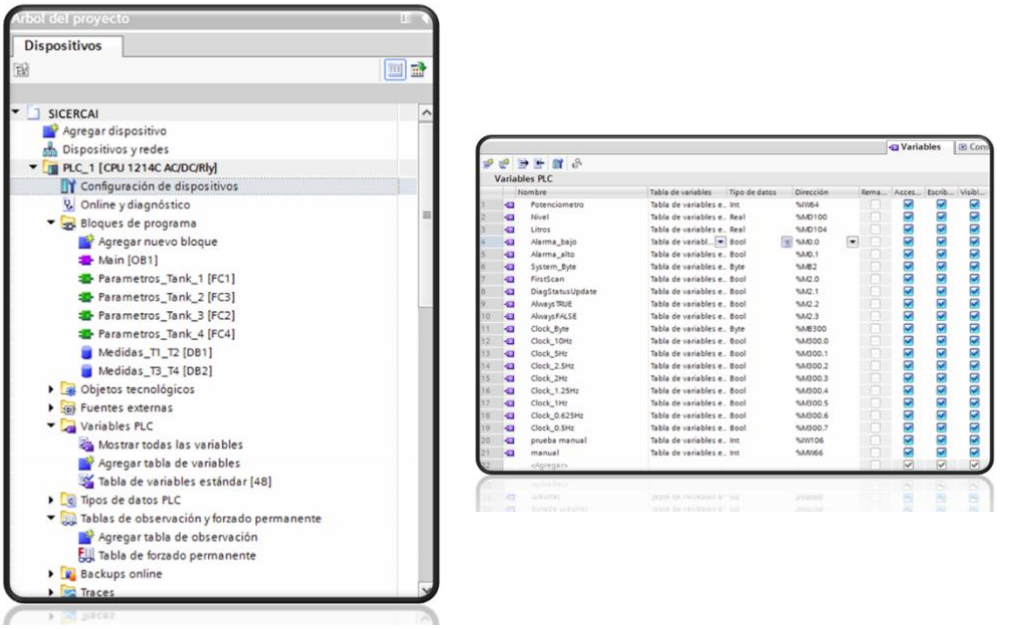


Figura 87: Imagen correspondiente al árbol de proyecto SICERCAI-2 y variables declaradas (TIA Portal).

En esta subsección se ha procedido a detallar los trabajos de ingeniería llevados a cabo para su utilización y la simulación de procesos que otorgan y dotan de capacidades realistas de despliegues bajo entornos operacionales y aplicados a las TO ejecutados en SICERCAI. Para ello, se han involucrado elementos de hardware, software y tecnologías de procesos.

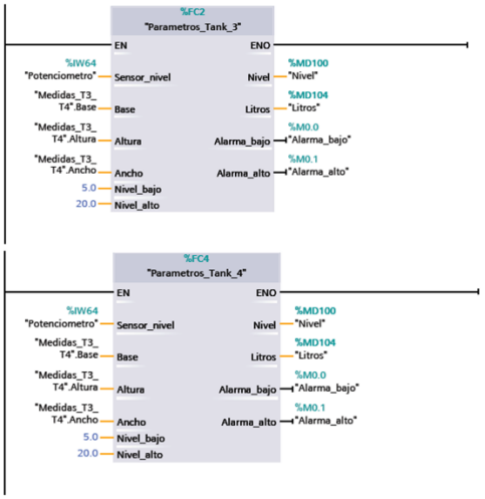


Figura 89: Contenido MAIN [OB1] del proyecto SICERCAI-2, segmentos 3 y 4.

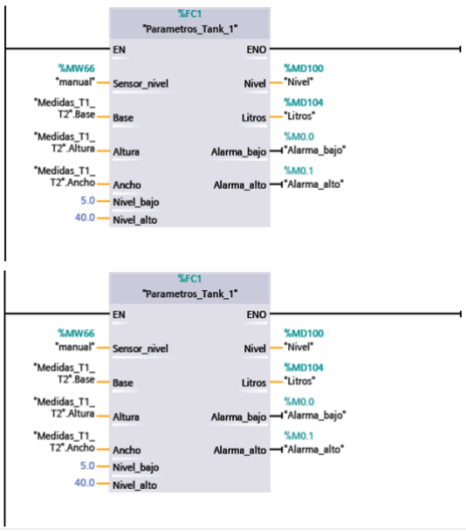


Figura 88: Contenido MAIN [OB1] del proyecto SICERCAI-2, segmentos 1 Y 2.

4.10. CVSS V3.0- Herramienta para la mejora de la ciber-resiliencia mediante SICERCAI

El contenido de sección trata sobre la metodología llevada a cabo y aplicada en SICERCAI para, conociendo una vulnerabilidad acreditada y debidamente documentada por una serie de entidades expertas en la materia, aprovechar las herramientas desplegadas en el sistema de conocimiento por experimentación real y obtener el conocimiento suficiente para mejorar las capacidades de prevención y resiliencia, llegando incluso a su prevención total [González S., 2020].

Se trata de poner a prueba la capacidad del nivel de tolerancia y absorción de un sistema como característica previa a un evento disruptivo en el sistema (ver Sección 4.2.1.1), propiedades y métricas de SCI resilientes.

El sistema común de evaluación y puntuación de vulnerabilidades (Common Vulnerability Scoring System, CVSS por sus siglas en inglés) [URL-108, 2021] es un marco abierto para comunicar las características y la

gravedad de las vulnerabilidades que afectan al software y elementos de hardware de distintos elementos en TI y TO [FIRST-CVSS SG., 2020], [Peter M., 2007], [González S., 2020].

Tras una detallada revisión bibliográfica de las herramientas de recopilación de infraestructuras TIC y ciberseguridad más relevantes, se ha optado para completar la instrumentación y optimizar la resiliencia mediante el uso de SICERCAI por el despliegue de un sistema con OpenVAS (Open Vulnerability Assessment Scanner, por su acrónimo en inglés) [URL, 109, 2021].

El escáner OpenVAS muestra los resultados de las vulnerabilidades y según el impacto en los sistemas las clasifica como: bajo, medio o alto, indicando el número de vulnerabilidades encontradas en cada categoría.

En el estudio desarrollado en "Obtaining high preventive and resilience capacities in critical infrastructure by industrial automation cells " [González S., 2020] se demuestra la estabilidad y capacidad ofrecida por OpenVAS ante la evaluación de sistemas OT tras la obtención de un análisis pormenorizado del uso de la herramienta. A su vez OpenVas cumple con los requisitos de comunicación y estandarización de todo lo relativo a la transferencias y codificaciones de cualquiera de las herramientas y servicios de seguridad utilizado por OVAL [URL- 110, 2021], estando asentado como productor de particularidades de los sistemas a evaluar.

Para cuantificar el riesgo de los sistemas empleados en SICERCAI por los diferentes usuarios han sido aplicadas las métricas identificadas en CVSS. La Tabla 17 facilita la comprensión de los términos utilizados.

A lo largo de esta sección para la estimación y como consecuencia, la obtención de capacidades de la mejora mediante la prevención y resiliencia, utilizando SICERCAI y CVSS, quedan implicados como elementos a valorar

cualitativa y cuantitativamente los niveles de vulnerabilidad, amenazas y riesgos de un entorno concreto recreado.

Del mismo modo y para entender el ámbito de aplicación y su justificación dentro del uso de CVSS de la variabilidad y dinamismo de los riesgos a los que se encuentran expuestos los sistemas, como recordatorio se clarifican y especifican las métricas listadas con anterioridad y que se encuentran involucradas en el sistema de evaluación de riesgos.

- ***Vulnerabilidad:*** Corresponde a una debilidad o fallo de un sistema en formación. Este fallo pone en riesgo la seguridad, permitiendo comprometer la integridad, la disponibilidad o la confidencialidad. Es necesario encontrarlos y eliminarlos lo antes posible. El tiempo transcurrido desde que se descubren hasta que se solucionan estos fallos se denomina "tiempo de exposición".
- ***Amenaza:*** Es una acción que se aprovecha de una vulnerabilidad, atacando un sistema de información. Por tanto, las vulnerabilidades son las condiciones y características que hacen que un sistema sea susceptible de sufrir amenazas.
- ***Riesgo:*** El riesgo es la probabilidad de que se produzca un incidente de seguridad. Es decir, la materialización de una amenaza, causando daños o pérdidas. Ser capaz de detectar las vulnerabilidades de software, hardware y firmware en los entornos de los sistemas de control industrial es primordial, ya que este riesgo es crítico para cualquier organización que opere un sistema TO e IoT. La identificación de estos riesgos puede ser difícil, así como su categorización y mitigación. El CVSS facilita de manera eficiente instrumentos para descubrir las principales características de las vulnerabilidades, proporcionando una clasificación cuantitativa y cualitativa que las cataloga como críticas, altas, medias y bajas, reflejando su gravedad inherente.

En resumen, el CVSS suministra tres importantes beneficios:

1. **Proporciona clasificaciones de vulnerabilidad estandarizadas.** Cuando una organización utiliza un algoritmo común para clasificar las vulnerabilidades en todas las plataformas de TI, puede aprovechar una única política de gestión de vulnerabilidades que define el tiempo máximo permitido para valorar y remediar una determinada vulnerabilidad.
2. **Facilita un marco de referencia abierto.** Los usuarios pueden confundirse cuando un tercero asigna una puntuación arbitraria a una vulnerabilidad. Con el CVSS las características individuales utilizadas para obtener una puntuación son transparentes.
3. **El CVSS permite priorizar los riesgos**. Cuando se computa la puntuación global, la vulnerabilidad se vuelve contextual para cada organización y ayuda a proporcionar una mejor comprensión del riesgo que supone esta vulnerabilidad para la organización [González S., 2020]. CVSS tiene tres tipos de grupos de métricas para evaluar los riesgos: *base, temporal y ambiental* (Tabla 17):
    a. ***Base.*** Representa las características intrínsecas y fundamentales de una vulnerabilidad que son constantes a lo largo del tiempo.
    b. ***Temporal.*** Abarca las características de una vulnerabilidad que cambian a lo largo del tiempo pero no entre entornos de usuario.
    c. ***Entorno.*** Constituye las características de una vulnerabilidad que son relevantes y únicas para un entorno de usuario concreto.

La interrelación y posterior análisis matemático de los datos ofrecidos por estas tres métricas dan como resultado una puntuación del sistema operacional.

El objetivo a alcanzar de esta catalogación es definir y especificar las características funcionales de una vulnerabilidad en concreto. Esto proporciona a los usuarios una representación clara e intuitiva de la

vulnerabilidad y una taxonomía común para la descripción de la misma. Los usuarios disponen de la posibilidad de invocar o no los grupos temporales y de entorno, proporcionando así una información contextual, que refleja con mayor precisión el riesgo para el medio considerado.

Cuando las métricas catalogadas y definidas en los párrafos anteriores se cuantifican con valores, la ecuación base calcula y proporciona una puntuación concreta, comprendida entre un rango de 0 a 10 mediante la creación de un vector de trabajo.

En la Tabla 17, se detallan algunos ejemplos de construcción de diferentes vectores.

Ejemplos de vectores asociados a los grupos de métricas	
Grupo Métricas	**Vector**
Base	AV: [L,A,N,P]/AC: [H,M,L]/Au: [M,S,N]/C: [N,P,C]/I: [N,P,C]/A: [N,P,C]
Temporal	E: [U,POC,F,H,ND]/RL: [OF,TF,W,U,ND]/RC: [UC,UR,C,ND]
Entorno	CDP: [N,L,LM,MH,H,ND]/TD: [N,L,M,H,ND]/CR: [L,M,H,ND]/ IR: [L,M,H,ND]/AR: [L,M,H,ND]

Tabla 17: Tipos de métricas en CVSS y vectores asociados.

El vector, que es una cadena de texto que contiene los valores asignados a cada métrica, facilita la comprensión de los agentes intervinientes para su evaluación. Se utiliza para comunicar exactamente cómo se obtiene la puntuación de cada vulnerabilidad, de modo que cualquiera pueda entender cómo se ha obtenido la puntuación y, si lo desea, confirmar la validez de cada métrica. Por lo tanto, es importante destacar que el vector debe mostrarse siempre con la puntuación de la vulnerabilidad. Los valores de estos vectores se muestran a continuación en la Tabla 18.

Calificación de las características e impacto de las vulnerabilidades informáticas (valor métrico y valor numérico)		
Métrica	**Valor Métrica**	**Valor Numérico**
Vector de Ataque / Vector de Ataque Modificado	Red	0.85
	Red Adyacente	0.62
	Local	0.55
	Físico	0.2
Vector de Ataque/ Vector de Ataque Modificado	Bajo	0.77
	Alto	0.44
Privilegio Requerido / Privilegio Modificado Requerido	Ninguno	0.85
	Bajo	0.62 (0.68 Sí Alcance/ Modificado, el Alcance está Cambiado)
	Alto	0.27 (0.50 Sí Alcance/ Modificado, el Alcance está Cambiado)
Interacción con Usuario / Interacción con Usuario Modificado	Ninguno	0.85
	Requerido	0.62
Confidencialidad, Integridad, Disponibilidad Impacto / Impacto Modificado	Alto	0.56
	Bajo	0.22
	Ninguno	0
Madurez del código del exploit	No Definido	1
	Alto	1
	Funcional	0.97
	Prueba de Concepto	0.94
	No Aprobado	0.91
Nivel de Corrección	No Definido	1
	No Disponible	1
	Solución	0.97
	Solución Temporal	0.96
	Solución Oficial	0.95
Informe de Confianza	No Definido	1
	Confirmado	1
	Razonable	0.96
	Desconocido	0.92
Requisitos de seguridad - Requisitos de confidencialidad, integridad y disponibilidad	No Definido	1
	Alto	1.5
	Medio	1
	Bajo	0.5

Tabla 18: Asociación entre métricas, valor de la métrica y valor numérico (CVSS).

La taxonomía de cada una de las métricas existentes en el vector para su formación está constituida por ***el nombre abreviado de la métrica*** seguido de ***":".***

Escala crítica valores cualitativos y cuantitativos	
Clasificación	**Puntuación CVSS**
Ninguno	**0**
Bajo	**0.1 - 3.9**
Medio	**4.0 - 6.9**
Alto	**7.0 - 8.9**
Crítico	**9.0 - 10.0**

Tabla 19: Escala de criticidad.

El vector enumera estas métricas en un orden predeterminado, utilizando el carácter ***"/"*** (barra oblicua) para separar las métricas. Si no es necesario utilizar alguna de las medidas de entorno o temporal, se le otorga el valor ***"ND"*** (no definido).

La aplicación de los parámetros y valores de las métricas concretas desarrolladas en el CVSS [FIRST, 2018] permite obtener un valor numérico concreto según la escala de valores especificada en la Tabla 19.

Los parámetros que intervienen para obtener la calificación de las características e impacto de las vulnerabilidades informáticas, corresponden a los detallados en la Tabla 18 definida anteriormente. El valor de la métrica debe elegirse en función de las características intrínsecas de cada sistema de las TO sometido al estudio. Esto implica que no todas las variables deben aparecer necesariamente.

4.10.1. Definición de ecuaciones utilizadas en CVSS

Para realizar los cálculos descritos en los apartados anteriores se utilizan tres tipos de ecuaciones [FIRST CVSS, 2020], [González S., 2020].

Es necesario destacar que los componentes individuales de las diferentes ecuaciones no han sido traducidos al español para evitar posibles errores y confusiones y así coincidir en su totalidad con las definiciones de FIRST[75] [URL- 111, 2021].

- ***Ecuación base:*** Las ecuaciones que definen y componen la llamada ecuación base se muestran en la Tabla 20.

Definición de la Ecuación Base
Definición de la Puntuación Básica
If (Impact sub score < = 0 else, 0) Scope Unchanged Roundup (Minimum [(Impact+Exploitability),10]) Scope Changed Roundup (Minimum[1.08×(Impact+Exploitability),10])
Sub-Puntuación de Impacto (Impact Sub-Score - ISC)
Scope Unchanged 6.42×ISCBase Scope Changed 7.52× [ISCBase−0.029] −3.25× [ISCBase−0.02]15 Where, ISCBase=1−[(1−ImpactConf) × (1−ImpactInteg) × (1−ImpactAvail)] Scope Unchanged Roundup (Minimum [(Impact+Exploitability),10]) Scope Changed Roundup (Minimum[1.08×(Impact+Exploitability),10])
Sub-Puntuación de Explotabilidad (Exploitability Sub-Score, ESS)
8.22 AttackVector x AttackComplexity × PrivilegeRequired × UserInteraction

Tabla 20: Definición de la ecuación Base (CVSS).

- ***Ecuación temporal:*** La definición completa de esta ecuación se muestra en la Tabla 21.

Definición de la Ecuación Temporal
Puntuación Temporal
Roundup (BaseScore × ExploitCodeMaturity × RemediationLevel × ReportConfidence)

Tabla 21: Definición de la ecuación Temporal (CVSS).

[75] FIRST (Forum of Incident Response and Security Teams) engloba al foro mundial de equipos de seguridad y respuesta a Incidentes. FIRST proporciona plataformas, medios y herramientas para que los equipos de respuesta a incidentes encuentren siempre el socio adecuado y colaboren de forma eficiente.

- ***Ecuación de Entorno:*** La composición completa correspondiente a esta ecuación se encuentra formada por tres componentes:
  - La definición de la puntuación de entorno.
  - La sub-puntuación de impacto modificada.
  - La sub-puntuación de explotabilidad modificada.

El valor de la métrica y los parámetros se definen y detallan a continuación en la Tabla 22.

Definición de la Ecuación de Entorno
Definición de la Puntuación de Entorno
If (Modified Impact 0 else, Sub score <= 0 If Modified Scope is Unchanged Roundup (Roundup (Minimum [× (M.Impact + M.Exploitability),10]) × Exploit Code Maturity × Remediation Level × Report Confidence) If Modified Scope is Changed Roundup (Roundup (Minimum [1.08 × (M.Impact + Exploitability),10]) × Exploit Code Maturity × Remediation Level × Report Confidence)
Sub-Puntuación de Impacto Modificada
If Modified Scope is Unchanged 6.42×[ISCModified] If Modified Scope is Changed 7.52 ×[ISCModified−0.029]-3.25×[ISCModified−0.02]15 Where, ISCModified = Minimum [[1−(1−M.IConf × CR) ×(1−M.IInteg × IR)×(1−M.IAvail × AR)],0.915]
Sub-Puntuación de Explotabilidad Modificada
8.22 × M.AttackVector × M.AttackComplexity × M.PrivilegeRequired × M.UserInteraction

Tabla 22: Definición de la ecuación de Entorno (CVSS).

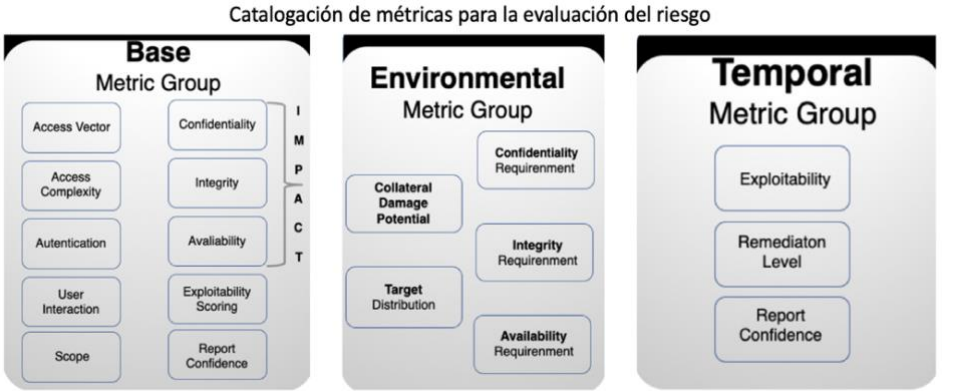


Figura 90: Catalogación de las métricas para la evaluación del riesgo (CVSS).

Tal y como se puede observar en la Figura 90, el conjunto de métricas, su catalogación y relaciones establecidas, siguiendo el marco de referencia CVSS V 3.0, se encuentran divididas en tres grandes grupos: *Base, Entorno y Temporales*, que a su vez se sub-dividen en diferentes categorías. En la siguiente sección se detallan individualmente el rol de cada uno de ellos dentro de la formación del vector base para el cálculo numérico de la vulnerabilidad sometida a estudio.

4.11. Caso de estudio y análisis tomado como premisa

Seguidamente se presenta el estudio materializado del caso específico que se ha planteado en el laboratorio donde se implementa SICERCAI utilizando la métrica de CVSS [González S., 2020].

En este caso de estudio se ha considerado como referencia una vulnerabilidad real y específica correspondiente al *PLC SIEMENS SIMATIC S7 1200*. En este caso del estudio en SICERCAI, después de utilizar el resultado obtenido a través de las métricas del CVSS, se debe tener en cuenta que los parámetros del estudio realizado han sido adaptados a un caso reproducido para su verificación en el sistema SICERCAI, no siendo el objetivo el análisis de una vulnerabilidad, sino su utilización como ejemplo práctico.

Esta vulnerabilidad ha sido previamente reportada y publicada oficialmente como:

- ***CVE 2016, 2846*** (Common Vulnerabilities and Exposures, CVS por sus siglas en inglés) [URL- 112,2016], [CVE, 2018].
- ***Advisory (CISA 16 075 01),*** Ciberseguridad y Agencia de Seguridad de las Infraestructuras, US CERT, Departamento de Seguridad Nacional [URL-113, 2016], [US CERT, 2016].
- ***SSA 833.048,*** asesoramiento de seguridad de SIEMENS por su correspondiente SIEMENS Product CERT [URL- 114, 2016], [SIEMENS Security Advisory, 2016].

SIEMENS es consciente de la vulnerabilidad del mecanismo de protección contra fallos en las antiguas versiones de firmware del SIMATIC S7 1200. Actualmente, este fabricante proporciona la solución para el producto correspondiente a la CPU SIMATIC S7 1200, V4.0 y posteriores, para así mitigar esta vulnerabilidad, recomendando en las páginas de soporte mantener el firmware actualizado en dichos dispositivos.

Como medida de seguridad universal, SIEMENS recomienda encarecidamente proteger el acceso a la interfaz web de red de la CPU S7 1200, con los mecanismos adecuados.

Según el paradigma recreado a través de SICERCAI (los cuales se encuentran recogidos en las Tablas 24, 25 y 26,) y tomando el vector base como vector inicial, los parámetros que se han tenido en cuenta para la demostración llevada a cabo han sido:

1. ***Vector de ataque (AV).***

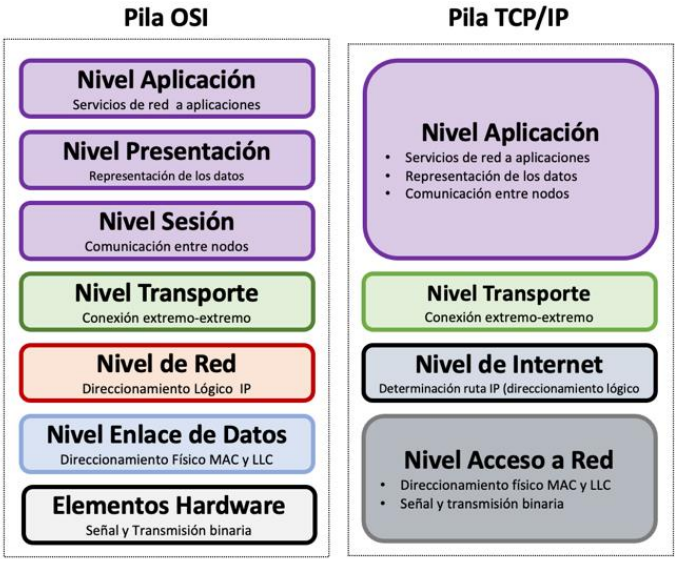


Figura 91: Representación gráfica pila OSI y pila TCP/IP.

Corresponde al primer parámetro, es decir, el origen del acceso, y que se desencadena en toda la red; una vulnerabilidad que se puede explotar con el acceso a la red significa que el software vulnerable está vinculado a la pila de la red (OSI[76], TCP/IP[77]) y el atacante no requiere acceso local a la red local. Para la comprensión de la diferencia entre OSI y TCP/IP, la Figura 91 representa gráficamente sus respectivas composiciones. Esa vulnerabilidad suele denominarse "vulnerabilidad de explotabilidad a distancia". Actualmente y tras un estudio publicado por "Help NetSecurity" en diciembre de 2020 [URL- 115, 2020] se destaca el descubrimiento de un total de 33 nuevas vulnerabilidades de seguridad

[76] El modelo de interconexión de sistemas abiertos (ISO/IEC 7498-1), más conocido como "modelo OSI", (*Open Systems Interconnection,* por sus siglas en inglés) es un modelo de referencia para los protocolos de red no siendo una arquitectura de red.

[77] El modelo TCP/IP es una descripción de protocolos de red y es usado para comunicaciones en redes y, como todo protocolo, describe un conjunto de guías generales de operación para permitir que un equipo pueda comunicarse en una red.

que afectan a cuatro pilas de TCP/IP de código abierto que son utilizados en millones de dispositivos desplegados en IoT (Internet of Things). Este estudio viene a remarcar la importancia del análisis de esta clase de vector de ataque, dado el notable aumento de este tipo de dispositivos, los cuales se despliegan en la industria 4.0 para el desarrollo de sus funcionalidades de manera eficiente.

2. ***Complejidad del acceso (AC).*** Su complejidad para el caso de estudio ha sido considerada baja. No existen condiciones de acceso especial ni circunstancias atenuantes a las mismas.
3. ***El producto afectado***. Suele requerir el acceso a una amplia gama de sistemas y usuarios, posiblemente anónimos y no fiables.
4. ***El ataque puede realizarse manualmente y requiere poca habilidad.*** También se sustenta por la escasa recopilación de información adicional necesaria para la ejecución del mismo. Carece de nivel de autenticación porque no es necesario para acceder a la explotabilidad de la vulnerabilidad tomada como base.
5. ***La vulnerabilidad explotada puede afectar a los recursos más allá de los privilegios de autorización que proporciona el componente vulnerable.*** De hecho esta capacidad se materializaría en la administración de los HMI conectados al PLC, bien directamente o a través de dispositivos de red industriales, siendo diferente el componente vulnerable y el componente implicado. La catalogación del nivel de confidencialidad involucrado ha sido considerado parcial como consecuencia directa de la considerable divulgación de la información.
6. ***El acceso a algunos archivos del sistema es posible*** pero el atacante no tiene control sobre lo que se obtiene, o bien el alcance de la pérdida o fuga de información se encuentra restringida. La evaluación de la explotabilidad se considera simplemente como una prueba de concepto,

ya que el ataque no se materializa en todas las situaciones y en paralelo, puede requerir modificaciones sustanciales por parte de un atacante experto.

7. ***La solución del proveedor mitiga completamente la vulnerabilidad*** y se encuentra disponible para su adhesión y actualización a los sistemas afectados, reduciendo drásticamente el tiempo de exposición a la vulnerabilidad. La vulnerabilidad pasa de vulnerabilidad de día 0 o "Zero Day"[78] a vulnerabilidad conocida. El fabricante ha emitido un parche oficial y una actualización disponible para su mitigación.
8. ***Credibilidad.*** Este parámetro se corresponde con la última medida de cuantificación a considerar dentro del vector base. Es la métrica correspondiente a la credibilidad. Ésta es calificación entre lo que se considera como la propia vulnerabilidad y la credibilidad de que haya sido reconocida por el fabricante del PLC en este caso SIEMENS.

Por último se detalla a continuación la trazabilidad de los cálculos realizados a través del vector base utilizado y representado (14) viniendo a aportar claridad sobre los resultados de las diferentes puntuaciones obtenidas del análisis específico de la vulnerabilidad referenciada como CVE 2016, 2846, y modificada para el caso de estudio concreto ejecutado.

Esta puntuación se corresponde exactamente con:

- *Puntuaciones de impacto: 9,8*
- *Puntuación base: 7,35*
- *Puntuación global: 8,575 (Alta)*

[78] Como su propio nombre indica, una vulnerabilidad de día cero o *Zero Day*, es un tipo de vulnerabilidad que acaba de ser descubierta y que aún no tiene un parche que la solucione.

La puntuación obtenida es la media aritmética de los valores aportados por los valores de impacto y la puntuación base. Esta vulnerabilidad se corresponde con una puntuación de **8,575,** y de acuerdo con la escala de criticidad de la puntuación del CVSS se corresponde con una catalogación **alta** (ver Tabla 19). A través de las Tablas 23,24 y 25, se indican los cálculos realizados para la resolución del caso de estudio tomado como ejemplo y de acuerdo con el vector base previamente discutido y detallado en:

$$\boldsymbol{AV}:N/\boldsymbol{AC}:L/\boldsymbol{Au}:N/\boldsymbol{UI}:N/\boldsymbol{S}:CC:P/\boldsymbol{I}:P/\boldsymbol{A}:N/\boldsymbol{E}:POC/\boldsymbol{RL}:OF/\ \boldsymbol{RC}:C \qquad \text{Expresión (14)}$$

Para una comprensión inequívoca de los parámetros, métricas y valores que forman las diferentes componentes del vector base, se han detallado cada uno de ellos en la Tabla 23.

Glosario de términos, métricas valores y parámetros.	
Valor Métrica	**Parámetros**
Attack Vector **(AV)**	Network**(N)**, Adjacent **(A)**, Local **(L),** Physical **(P)**
Attack Complexity **(AC)**	Low **(L)**, High **(H)**
Privileges Required **(PR)**	None **(N)**, Low **(L)**, High **(H)**
User Interaction **(UI)**	None **(N)**, Required **(R)**
Scope **(SC)**	Unchanged **(U)**, Changed **(C)**
Confidentiality Impact **(CI)**	High **(H)**, Low **(L)**, None **(N)**
Integrity Impact **(II)**	High **(H)**, Low **(L)**, None **(N)**
Availability Impact **(AI)**	High **(H)**, Low **(L)**, None **(N)**
Exploit Code Maturity **(ECM)**	Not Defined **(X)**, High **(H)**, Functional **(F)**, Proof-of-Concept **(P)**, Unproven **(U)**
Remediation Level **(RL)**	Not Defined **(X)**, Unavailable **(U)**, Workaround **(W)**, Temporary Fix **(T)**, Official Fix **(O)**
Report Confidence **(RC)**	Not Defined **(X)**, Confirmed **(C)**, Reasonable **(R)**, Unknown **(U)**
Security Requirements **(SR)**	Not Defined **(X)**, High **(H)**, Medium **(M)**, Low **(L)**

Tabla 23: Glosario de términos usados en las ecuaciones.

Cálculos operacionales llevados a cabo (Tablas 24, 25 y 26):

Base-Explotabilidad-Ecuaciones de entorno		
Métrica Base	**Evaluación**	**Puntuación**
Access Vector	[Network]	(0.85)
Access Complexity	[Low]	(0.77)
Authentication	[None]	(0.85)
User Interaction	[None]	(0.85)
Scope	[Changed]	-------
Confidentiality Impact	[Partial]	(0.34)
Integrity Impact	[Partial]	(0.34)
Availability Impact	[None]	(0.00)
Exploitability Scoring	[POC]	(0.94)
Remediation Level	[Official Fix]	(0.95)
Report Confidence	[Confirmed]	(1.00)

Tabla 24: Ecuaciones de entorno (Métrica base).

Base-Explotabilidad-Ecuaciones de entorno		
Métrica Temporal	**Evaluación**	**Puntuación**
Exploitability	= 10.41 x (1-(1-0.66 x 1) x (1-0.66 x 1) x (1-0.0 x 0.5))	== 9.80
AdjustedBase	= ((0.6 x 9.8) + (0.4 x 0.94)–1.5) x 1.176	== 7.35
AdjustedTemporal	= (7.35 x 0.9 x 0.87 x 1.0)	== 5.75
EnviroScore	= round ((5.75 + (10-5.75) x 0.5) x 0.25)	== (0.0 - 2.0)

Tabla 25: Ecuaciones de entorno (Fórmula base).

Base-Explotabilidad-Ecuaciones de entorno	
Fórmula Base	**Puntuación**
Impact 10.41 x (1-(1-ConfImpact) x (1- IntegrImpact) x (1-AvailImpact)	== 5.80
BaseScore (((0.6 x Impact) + (0.4 x Exploitability) - 1.5) x f (impact)	== 7.04
F (impact)	== 1.17
ISCBase = 1- [(1-0.34) x (1-0.34) x (1-0)]	== 0.56
Impact Sub Score= 7.52 x [ISCBase – 0.029] -3.25 x [ISCBase – 0.02]15	== 0.74
Exploitability = 20 x [(Access Vector) x (Access Complexity) x (Authentication)]	== 10.0
Exploitability Sub Score = 8.22 x AccesVector x AccessCplex x UserInteract	== 4.57

Tabla 26: Ecuaciones de entorno (Métricas temporales).

4.12. Resultados y conclusiones

En la investigación llevada a cabo utilizando SICERCAI se ha presentado el desarrollo de un nuevo concepto de simulación de procesos en entornos industriales a través del aprendizaje mediante la experimentación real, aprovechando los avances en el mundo de la informática y comunicaciones.

En la actualidad, con el aumento de la presencia de las TI en el área del control de las TO, los sistemas industriales están expuestos a un gran número de nuevas amenazas cibernéticas, como así ha quedado detallado a lo largo del Capítulo 3.

Dado el trascendente papel que desempeñan estas infraestructuras y servicios esenciales para el normal desarrollo y convivencia de la sociedad, y como así ha quedado patente tras la realización del profundo análisis del estudio del arte en materia de ciberseguridad industrial, es momento de reflexionar sobre la actualidad y la tendencia futura de los ciberataques en

las IC. Los ciber-delincuentes dirigirán sus esfuerzos hacia la obtención de ataques exitosos focalizados en estas infraestructuras [Genge B., 2015].

Se debe desechar la idea de que la *"seguridad por oscuridad"* es un método válido para la protección contra este tipo de ataques. Por ello, es muy importante estar preparado para posibles eventualidades a través de "prácticas y pruebas" [Stergiopoulss G., 2015], obteniendo así un alto grado de resiliencia [Roldan M., 2017], [Chaves A., 2017] y, al mismo tiempo, un alto grado de madurez ante los nuevos vectores que darán acceso a los ciberataques en los sistemas de control industrial.

La mejor defensa contra estos nuevos desafíos es el entrenamiento. A su vez, la puesta en práctica de los conocimientos teóricos sin el riesgo que supone la puesta en práctica de estos análisis en las plantas de producción favorece la experimentación y la ampliación de los puntos de vista.

Estas cualidades prácticas de mejora de las capacidades preventivas y resilientes se encuentran garantizadas por el sistema SICERCAI, ya que permite elegir cómo diseñar el entorno real que se va a simular, incluyendo cada uno de los componentes que intervienen en los sistemas de control:

- *Sistemas operativos* (en el lado de la red de control y administración).
- *Software de programación* específico para componentes industriales (PLC, electrónica de red, sistema SCADA).
- *Conexión a la Célula de Automatización Industrial* (CAI-1).
- *Sistema de análisis de tráfico de red*.
- *Herramientas de monitorización y análisis de vulnerabilidades* mediante OpenVAS. La verdadera versatilidad del sistema está garantizada por la alta capacidad de adaptación para la incorporación de tantas CAI como fabricantes de sistemas de control y automatismos industriales existentes.

- El uso del framework CVSS en su versión 3.0, ante la situación del conocimiento de una vulnerabilidad con sus métricas de impacto y criticidad, como así ha sido demostrado en el presente capítulo, oferta la capacidad de recrear los paradigmas planteados por los usuarios de SICERCAI, otorgando consecuentemente capacidades de previsión ante desarrollos incorrectos, ejecuciones, configuraciones y tratamientos de las TI junto a las TO. La versión 3.1 en concreto, resalta que el CVSS está diseñado para medir la severidad de una vulnerabilidad y, por ello, no debe ser utilizado como única herramienta para evaluar el riesgo. El reciente documento de especificaciones de CVSS correspondiente a la versión 3.1, establece con claridad que la puntuación base de CVSS (*Base Score*) representa sólo las características intrínsecas de una vulnerabilidad. Estas son constantes en el tiempo y comunes a los distintos entornos de usuario. Por este motivo y para poder realizar un análisis de riesgos metódico, esta puntuación base debe complementarse con un análisis contextual aprovechando las métricas temporales y del entorno, y con otros factores externos no contemplados por el CVSS como exposición y amenaza.

La Figura 92 describe la modificación del nuevo modelo de puntuación, por lo que se produce una reformulación de las ecuaciones necesarias para su uso. Para ayudar a clarificarla, en la composición de los elementos para sustentar la definición de la métrica, se introducen dos variantes que se corresponden con la variabilidad o no de si el impacto ejercido escapa del elemento vulnerable. A su vez la nueva cadena del vector base resultante de CVSS V 3.1 [URL- 116, 2021] quedaría modificada respecto al utilizado en las pruebas de concepto llevadas a cabo con SICERCAI como se observa en la ecuación 15, y como consecuencia del nuevo método de puntuación.

*CVSS: 3.1 / **AV**:x/**AC**:x/**PR**:x/**UI**:x/**S**:x/**C**:x/**I**:x/**A**:x*
*EXT: 1.0 /**NEW1**:VAL1/**NEW2**:VAL2* (15)

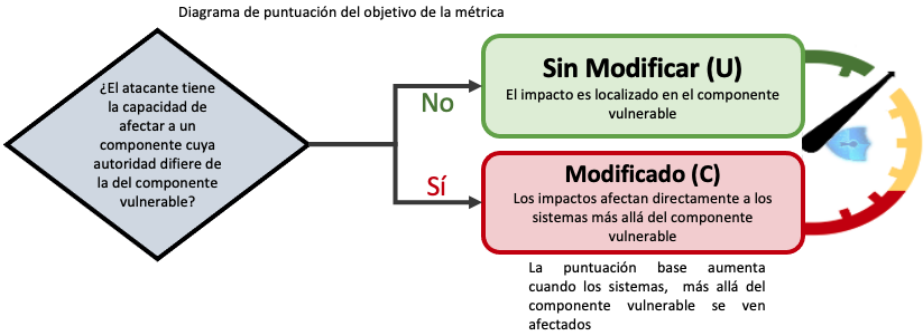


Figura 92: Diagrama de puntuación sobre el objetivo de la métrica.

Es importante recalcar que se ha llevado a cabo este análisis utilizando CVSS V 3.0, por ser el caso más adecuado ante la vulnerabilidad/es existentes en elementos industriales correspondientes al periodo de tiempo 2015-2018, segmento temporal donde se encuadra la vulnerabilidad con identificador CVE 2016, 2846, utilizada para su evaluación. De igual manera, la capacidad de proporcionar el software involucrado en estas redes, permite una mayor calidad en el análisis de vulnerabilidad y por consiguiente su recreación en entornos SandBox[79], otorgando esta cualidad SICERCAI.

En [Zhang Y., 2020] se pone de manifiesto la importancia del despliegue de este tipo de arquitecturas, dada su importancia ante la eventualidad de someter examen y probar elementos maliciosos del tipo ransomware[80]

[79] En ciberseguridad, sandbox significa aislamiento de procesos. Es decir, un entorno en el que aislar un programa o archivo infectado (o sospechoso de serlo) para evitar que el virus se extienda o para estudiar su comportamiento y desarrollar soluciones en consecuencia.

[80] El *ransomware* es un tipo de malware que se introduce en los equipos y dispositivos móviles impidiendo el acceso a la información, generalmente cifrándola, y solicitando un rescate (*ransom*, en inglés) para que vuelva a ser accesible.

industrial como EKANS[81] y Snake[82]. En consecuencia, la principal contribución de esta investigación, materializada en SICERCAI, es la provisión de un marco seguro que proporciona ayuda para obtener resultados mediante análisis que demuestren el verdadero estado de madurez de una arquitectura de ensayos industriales, que los usuarios desplegarán de acuerdo con sus necesidades de investigación, análisis o ejecución [URL- 117, 2021].

4.13. Resumen

En este capítulo han sido desarrolladas y mostradas las contribuciones de SICERCAI para la mejora de la ciberseguridad y ciber-resiliencia de los SCAI.

En primer lugar se argumentaron las premisas que justifican por qué debe jugar un papel clave la protección cibernética de los sistemas y automatismos industriales y, por consiguiente, su ciber-resiliencia, dando como resultado la motivación de la creación y puesta en funcionamiento de SICERCAI.

Seguidamente, y con el fin de obtener el punto de partida de las pruebas a las que fueron sometidos los entornos desplegados para su evaluación, han sido detallados exhaustivamente todos y cada uno de los componentes que forman SICERCAI.

[81] El ransomware EKANS surgió a mediados de diciembre de 2019, y Dragos publicó un informe privado para los clientes de Dragos WorldView Threat Intelligence a principios de enero de 2020. EKANS presentaba una funcionalidad adicional para detener por la fuerza una serie de procesos, incluyendo múltiples elementos relacionados con las operaciones de Sistemas de Control Industrial.

[82] El ransomware SNAKE intenta extorsionar a sus víctimas encriptando sus archivos, dejando a los afectados con pocas opciones. La lista de procesos que utiliza es similar a una variante del ransomware MegaCortex que surgió como amenaza en 2019.

Esta disociación de componentes viene a contribuir y a facilitar el entendimiento de los detalles técnicos individuales y su aporte a la globalidad del sistema, particularizando cada uno de los roles asumidos por cada subsistema componente, definiendo en paralelo sus aportes a la confluencia de las TI y TO.

Acto seguido, y partiendo de la globalidad de la arquitectura planteada, fueron especificados ciertos parámetros y ejecutados a su vez varios ejemplos, los cuales fueron creados a través de software de ingeniería para las TO, con el fin de recrear un sistema real desplegado en nuestra sociedad, un sistema de gestión de tráfico rodado y peatonal.

Tras obtener las características técnicas y sus requisitos operacionales, el sistema a evaluar, y habiendo llevado a cabo un planteamiento previo de las potenciales problemáticas asociadas a un entorno en concreto, se centraron los esfuerzos en la evaluación del potencial impacto de un riesgo latente, optando para ello por la elección y uso del CVSS como sistema que proporciona una puntuación en función al impacto que una vulnerabilidad concreta podría llegar a tener en caso de ser explotada.

Con ese fin, se toma como referencia y elemento base una vulnerabilidad específica de un autómata programable de la familia SIMATIC S7 modelo 1200, con la que se pone de manifiesto las capacidades de la variabilidad de las puntuaciones del impacto de dicha vulnerabilidad tras aplicar SICERCAI, confiriendo claramente mejoras en la ciberseguridad y ciber-resiliencia de los sistemas.

Finalmente se estudian los factores que influyen en la variabilidad de los entornos, caracterizandolo para el ejemplo concreto elegido para tal fin.

Capítulo V

Búsqueda de vulnerabilidades en sistemas de generación y distribución eléctrica (CCDCoE)

5. Introducción

Tras la descripción en los capítulos previos de los principales aspectos y problemáticas que influyen y, que a su vez, han emergido en los entornos operacionales mediante el uso de las tecnologías de la información, se ha concluido con el análisis de dichas situaciones mediante la creación, la implementación y la puesta en funcionamiento de SICERCAI como un modelo de banco de pruebas.

Por otro lado, y ya centrados en el sector energético como sector especialmente crítico, junto con el desarrollo y el despliegue de subestaciones inteligentes basadas en la norma IEC 61850[83], cada vez surgen más vulnerabilidades de ciberseguridad en los sistemas de control y adquisición de datos (SCADA) [Rodolfile N., 2019], [Rosas W., 2020]. Como respuesta a la aparición de estas vulnerabilidades de ciberseguridad en las subestaciones inteligentes, se torna indispensable la realización de pruebas que permitan la experimentación entre las diferentes arquitecturas desplegadas, las cuales certifiquen y muestren las posibles carencias en materia de ciberseguridad de esos entornos.

En este sentido, y para completar el trabajo presentado en esta Tesis, en este capítulo se refleja la investigación en la que participé como colaborador durante una estancia de investigación en Tallin (Estonia).

[83] IEC 61850 es un estándar internacional de comunicación originariamente dirigido a los procesos de automatización, control y protección de los sistemas de las subestaciones permitiendo interoperabilidad entre fabricantes.

El capítulo muestra los resultados obtenidos en esa colaboración en la que se evaluó una infraestructura de red, asociada a la generación y el transporte eléctrico, poniendo el foco en la importancia que se debe otorgar a la ciberseguridad de este tipo de instalaciones.

El contenido principal de este capítulo explica al detalle el trabajo desarrollado en el Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN sito en Tallin (Estonia) (NATO Cooperative Cyber Defence Centre of Excellence, CCDCoE[84], por sus siglas en inglés).

En el CCDCoE, a modo de laboratorio de pruebas y evaluación, se encuentran desplegados varios sistemas, terminales y dispositivos electrónicos existentes en el segmento de la generación y transporte eléctrico, ostentando una naturaleza de ámbito completo y realista. Tras un primer trabajo de investigación y el posterior análisis de los datos, se muestran los resultados obtenidos, los cuales han otorgado la posibilidad de llevar a cabo pruebas de extremo a extremo mediante intrusiones en la red de comunicaciones, mostrando las vulnerabilidades tecnológicas halladas en ciberseguridad y en consecuencia, los potenciales impactos de los ciberataques en las subestaciones inteligentes basadas en la norma IEC 61850. En paralelo a ello, se perseguía el hallazgo de vulnerabilidades de "día 0" en plataformas y dispositivos de control industrial en las áreas especificadas anteriormente, estando involucrados los principales fabricantes a nivel mundial y que se encuentran, a su vez, desplegados en IC.

[84] El CCDCoE como centro de ciber-defensa acreditado por la OTAN, ostenta la misión de apoyar a los países miembros y a la OTAN con una experiencia interdisciplinaria única en el campo de la investigación, la formación y los ejercicios de ciber-defensa, cubriendo las áreas de tecnología, estrategia, operaciones y derecho.

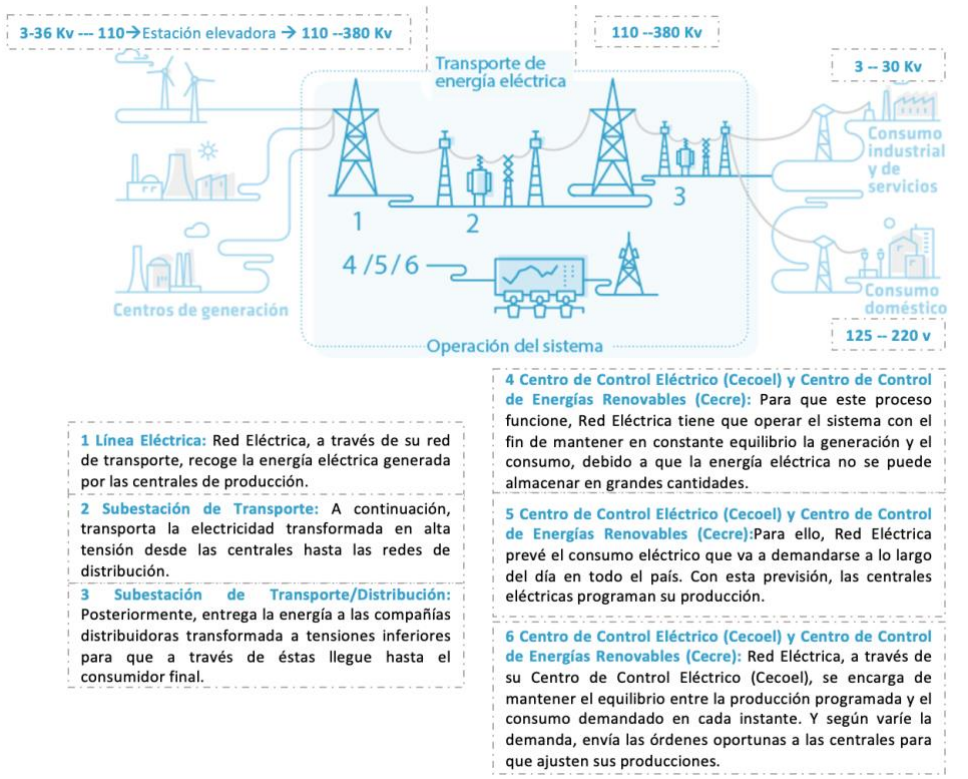


Figura 93: Etapas del recorrido de la energía eléctrica desde puntos de generación hasta su consumo final (modificada de la fuente original: www.ree.es).

Ya para concluir la introducción de este capítulo y para proporcionar claridad sobre el tema a tratar, la Figura 93 representa gráficamente las diferentes etapas involucradas en el camino que recorre la energía eléctrica desde el momento de su generación hasta su consumo, tanto en el ámbito doméstico como en el industrial. Las etapas representadas se subdividen en dos grandes conjuntos de actividades y que se corresponden y agrupan en *transporte de la energía* (puntos 1, 2 y 3) y *operación del sistema* (puntos 4, 5 y 6).

El estudio presentado ha sido desarrollado en el segmento de los SACI desplegados en la parte de la operación del sistema.

5.1. Contenido del estudio llevado a cabo en el CCDCoE

Figura 94: Pila OSI (Open Systems Interconnection, sistema abierto de interconexión).

Dada la envergadura del proyecto, así como la variedad de la tecnología desplegada, cuya propiedad le corresponde al CCDCoE, las líneas de trabajo fueron fijadas y acotadas de la siguiente manera:

1. **Análisis de la arquitectura del estándar de comunicación IEC 61850.** El estándar IEC 61850, desarrollado por la Comisión Electrotécnica Internacional (International Electrotechnical Commission, IEC, por sus siglas en inglés) [UR-118, 2021], define una serie de protocolos de comunicación utilizados entre los distintos dispositivos que forman parte de las subestaciones eléctricas. Estos protocolos se corresponden con:
    - **Sampled Measured Values (SMV[85]).** Está diseñado para proporcionar una transmisión rápida de valores de medición,

[85] El SMV es un método utilizado para pasar las muestras medidas de las unidades que recogen las medidas (analógicas-digitales), como los TC, los TV o las E/S digitales compartidas entre los dispositivos IED.

protección y control. Su funcionamiento se produce a través de Ethernet (capa 2 del modelo OSI, Figura 94) y los mensajes son encapsulados como multicast[86], siguiendo una estructura de *emisor – suscriptor*, donde el emisor envía los datos a todos los equipos de la red y cada equipo se suscribe a los datos para acceder a los mismos.

- **Simple Network Time Protocol (SNTP[87]).** Para la sincronización del reloj de los dispositivos se utiliza el protocolo SNTP. Como su propio nombre indica, es una versión simplificada del protocolo NTP, utilizado en equipos que no necesitan la funcionalidad completa del protocolo. Para la transmisión de los mensajes SNTP se utiliza el protocolo UDP (Capa 4 del modelo OSI).
- **Manufacturing Message Specification (MMS[88]).** El protocolo envía sus mensajes para las comunicaciones cliente/servidor a través de conexiones TCP (Capa 4 del modelo OSI, Figura 94). Es utilizado para el intercambio de datos de aplicación y de parámetros de configuración de los dispositivos o datos de monitorización. Así, la comunicación entre los equipos y el SCADA o el SAS, se denomina "MMS", [Mashima D., 2021].
- **Generic Substation Events (GSE)**. Son un modelo de control definido según la norma IEC 61850 [URL- 119, 2021], el cual proporciona un mecanismo rápido y fiable de transferencia de datos

[86] La multidifusión IP o multicast, es un método en comunicaciones de redes de ordenadores, por el que se transmiten un conjunto de datagramas IP a un grupo de receptores

[87] El simple network time protocol, abreviado como SNTP, es un protocolo de la familia de protocolos de internet que se utiliza para sincronizar los relojes de sistemas informáticos en redes

[88] El estándar MMS fue desarrollado específicamente para aplicaciones industriales; está especificado según ISO 9506 y sirve para el intercambio de datos en ambientes de producción. Redes de control utilizan el protocolo MMS y una pila reducida del modelo OSI con el protocolo TCP/IP en la capa de transporte/red, y Ethernet o RS-232C como medio físico.

de eventos a través de redes de subestaciones eléctricas. Cuando se implementa, este modelo asegura que el mismo mensaje de evento sea recibido por múltiples dispositivos físicos utilizando servicios de multidifusión. Este modelo a su vez se subdivide en:

- **Generic Object Oriented Substation Events (GOOSE).**[89]
- **Generic Substation State Events** (**GSSE,** actualmente en desuso).

2. **Configuración, despliegue y posterior análisis del comportamiento de las redes industriales creadas**. En el laboratorio se desplegaron un total de 24 Remote Terminals Units (RTU[90]) del fabricante SIEMENS, modelo SICAM A800 y sus 24 sistemas SCADA asociados, con sistemas de gestión Spectrum V 5.0.[91] [URL- 120, 2021].
3. **Recreación de un escenario real de generación eléctrica en la parte de transporte**. A las arquitecturas generadas se les asoció 24 dispositivos electrónicos inteligentes (Intelligence Electronics Devices, IED[92], por sus siglas en inglés) de diferentes fabricantes: *SIEMENS, ABB, Schneider Electric, ARCTEQ, TOSHIBA, WOODWARD, SCHWEIZER, General Electric, BASLER, e ICE*. De esta manera, se pudo recrear el escenario real involucrado en las estaciones de generación eléctrica y en la parte de su transporte.

[89] En entornos IEC 61850, los mensajes GOOSE (eventos de subestación genéricos orientados a objetos) son el mecanismo utilizado para distribuir información de estado. Se publican como mensajes de multidifusión sin estar dirigidos a ningún receptor en particular.

[90] Una Unidad Terminal Remota (UTR o, más conocida por sus siglas en inglés, RTU) es un dispositivo basado en microprocesadores, el cual permite obtener señales independientes de los procesos y enviar la información a un sitio remoto donde se procese.

[91] Los sistemas Spectrum (en sus diversas versiones) corresponde con un software específico de gestión en Smart Grid. Es un sistema propietario de SIEMENS.

[92] Los IED reciben datos de los sensores y diversos dispositivos eléctricos, y pueden informar de los comandos de control, tales como interruptores que se disparan cuando se detectan voltajes, corrientes o frecuencias anómalas, cuando se suceden las variaciones por el aumento o niveles de tensión inferior para mantener el nivel deseado.

4. **Búsqueda de vulnerabilidades de día 0,** en la arquitectura anteriormente descrita. Esta búsqueda se llevó a cabo involucrando el propio protocolo de comunicaciones (GOOSE y MMS), junto con software de terceros implicado en la configuración de los IED y RTU, así como en los propios elementos de hardware implicados en la arquitectura.

Para el correcto desarrollo de la investigación dentro del proyecto planteado, se hizo uso de software específico para la auditoría de redes, configuraciones y sistemas en general (WireShark, SO Kali-Linux, IEDScout Software V5.00 [URL- 121, 2021], y herramientas de fuzzing[93] [Tengfei T., 2017], las cuales auxiliaron a la investigación y facilitaron una profundización en el conocimiento de los protocolos de comunicación GOOSE y MMS, ampliamente desarrollados e implantados en la rama de la generación y distribución eléctrica.

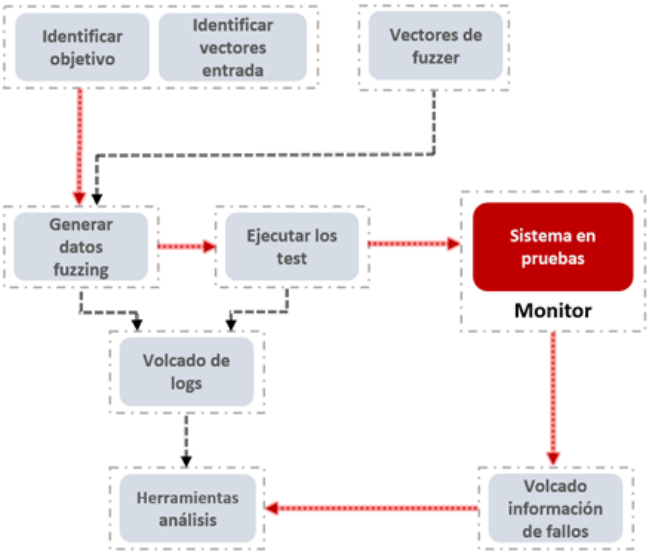


Figura 95: Diagrama de funcionamiento herramientas de fuzzing (modificada de la fuente original: INCIBE-CERT).

[93] Se conoce como *fuzzing* o técnicas de *fuzzing* al conjunto de pruebas de caja negra que permiten descubrir errores en los programas o protocolos mediante la introducción de datos al azar, inválidos y malformados.

La Figura 95 se corresponde con el diagrama de funcionamiento genérico de un proceso de pruebas aplicando técnicas de fuzzing, en donde quedan debidamente identificadas las principales acciones que se llevan a cabo en cada uno de los procesos.

5.2. Redes eléctricas inteligentes smart grid

Para poder obtener una visión global del concepto de las redes eléctricas inteligentes de nueva generación, denominadas *"smart grid" (SG),* que desde comienzos del siglo XXI las compañías eléctricas han venido desplegando, se hace necesaria una breve descripción de las mismas. Este tipo de redes proporcionan un referente de modernidad focalizado en la red de gestión de la demanda y del consumo eléctrico. En esta subsección se procede a identificar los principales componentes necesarios para la creación de una infraestructura de medición avanzada (Advanced Metering Infrastructure, AMI, por sus siglas en inglés) y que, en paralelo, permita identificar todas aquellas áreas que han servido como base para el desarrollo de la investigación descrita a lo largo de este capítulo [Kumar V., 2021].

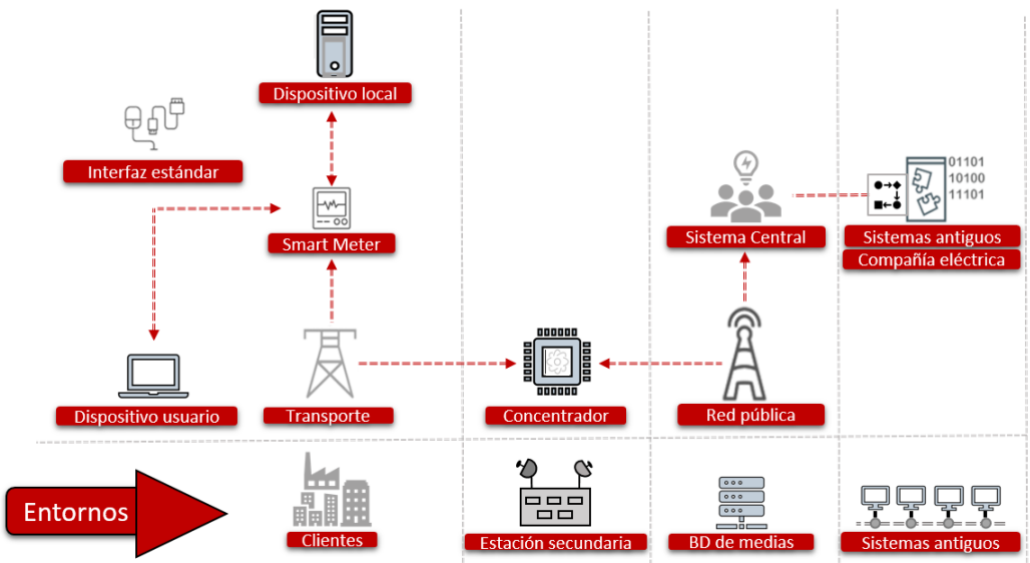


Figura 96: Principales componentes de una infraestructura de medición avanzada (AMI).

La Figura 96, representa de modo esquemático los principales componentes e interfaces partícipes en una AMI. Como se puede observar de la imagen, se corresponde con una infraestructura cuya dedicación se corresponde con los sistemas, que se encargan de medir, recolectar y analizar el uso de la energía, interactuando a su vez con los dispositivos medidores inteligentes dispuestos en los puntos de consumo (contadores inteligentes o smart meter[94])

5.3. Importancia de la ciberseguridad en sistemas de generación y distribución eléctrica

Como se ha sugerido en capítulos anteriores, la ciberseguridad en los SCI juega un papel importantísimo debido a la modernización extrema que están sufriendo los entornos industriales en íntima dependencia con las TI.

Para venir a resaltar aún más esta dependencia, una perturbación del suministro eléctrico puede dejar sin energía durante un determinado tiempo a una determinada zona con las consiguientes incomodidades, pero sin dejar de ser un posible hecho anecdótico. Pero si esa interrupción se prolonga en el tiempo, la perturbación de la prestación puede impactar en servicios ofrecidos por otros sectores y por las propias IC de forma grave y con consecuencias extremas.

El efecto de una caída en cascada de los servicios ante una disrupción, puede afectar no sólo a otros sectores estratégicos/críticos, sino también a otras redes e incluso a otros países, dada la interconexión de las mallas energéticas. Dentro del ámbito de aplicación de este efecto en cascada, debe resaltarse la estrecha relación de interdependencia que existe entre las

94 Un contador inteligente o smart meter, se trata de un contador avanzado de elctricidad que calcula el consumo eléctrico de forma detallada y que se considera pieza clave en las infraestructuras smart grids.

smart grid y las redes de telecomunicaciones, ya que, si estas mallas inteligentes ofrecen a las redes la energía necesaria para su funcionamiento, las infraestructuras de telecomunicaciones son también necesarias para el buen funcionamiento de las smart grids, y esta reciprocidad, será cada vez más dependiente a medida que la tecnología, como, por ejemplo, la comunicación 5G, vaya implantándose en el mundo industrial [URL- 122, 2020], [Shrestha M., 2020], [Tweneboah-Koduah S., 2020].

A la importancia, que ya el sector energético ostenta para la economía y sociedad a nivel mundial, le corresponde ser añadida las adaptaciones y modernizaciones de las propias redes energéticas. El planeta está enfrentándose a retos de gran calado, como son la descarbonización mediante la reducción al máximo de los combustibles fósiles, la descentralización mediante tecnologías de control disgregadas y la digitalización en toda la cadena de valor, desde la generación y la distribución hasta llegar al consumidor.

La generación energética renovable y distribuida en baja tensión, (mostrada en el punto 3 de la Figura 93), la energía solar fotovoltaica, el almacenamiento y el vehículo eléctrico, conectados todos ellos en los puntos de consumo, son auténticas directrices recalcadas dentro del sector. A lo anteriormente expuesto, hay que añadir el nuevo rol de los propios consumidores, que viene definido no sólo por el consumo energético, sino también por la propia producción e inyección al torrente eléctrico de lo aportado, lo que involucra varios modelos de cambios en la relación con las compañías y en el modelo de negocio de las distribuidoras, convirtiéndolas en facilitadoras de mercado que explotan la gran cantidad de información de la que disponen y ofrecen nuevos servicios de alto valor añadido [URL- 123, 2019].

Es destacable la incorporación de los dispositivos inteligentes del IoT así como del IIoT, puesto que el volumen de incorporación de estos elementos a las redes eléctricas inteligentes aumenta día a día. En paralelo a esta masiva incorporación se está produciendo un aumento desmesurado del consumo eléctrico. Ese aumento repercutirá en el consumo mundial, creciendo hasta en un 48% para el año 2040 [URL-124, 2021]. Esta nueva situación precisa de un equipamiento específico para integrar la infraestructura eléctrica, como son las estaciones y los puestos de recarga, con la generación eólica y/o la distribuida con paneles fotovoltaicos domésticos, entre otros.

Y puesto que el incremento de la superficie de exposición conllevará un aumento del ciber-riesgo de las smart grids, se hace necesario considerar su seguridad desde el diseño y en todos los entornos operacionales (software de ingeniería, arquitecturas remotas, comunicaciones, etc.), para así minimizar el riesgo ante ataques masivos desde dispositivos IoT provenientes, por ejemplo, de los sistemas de control de la humedad, ventilación y climatización (Heating, Ventilating and Air Conditioning, HVAC, por sus siglas en inglés) instalados en hogares y en los entornos operacionales y los grandes centros de computación de las diferentes instituciones.

5.4. Del enfoque eléctrico al enfoque de datos y control

Tras haber realizado una exposición de la parte más física de las smart grid, así como la exposición de la cadena de valor de la electricidad al uso, se deduce que es necesario un control y monitorización permanente de las mismas. Esta situación se encuentra justificadamente motivada por las siguientes exigencias:

- *Permanecer estables frente a la demanda y la generación energética.*
- *Aseguramiento de la disponibilidad energética.*

- *Garantía de la seguridad del sistema en general, y de los subsistemas y las operaciones en particular.*
- *Inspección de eventos propiciados por la operación*.

Los sistemas SCADA ostentan la particularidad de poder realizar el control y la monitorización de todos estos aspectos a través de la captura de la información de todos y cada uno de los dispositivos desplegados. Como se puede observar en la Figura 97, existe una parte muy importante de estos sistemas SCADA concentrada en el segmento del consumo en donde proliferan las transmisiones *datos + energía.*

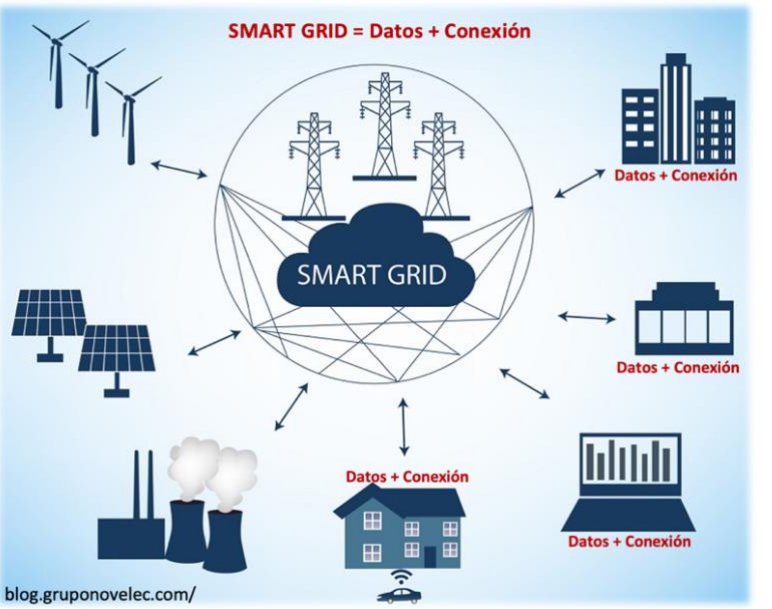


Figura 97: Esquema-composición de una smart grid (modificada de la fuente original: blog.gruponovelec.com).

Es de suma importancia resaltar que el control en la parte operacional de las smart grid se encuentra al mismo nivel por su propia definición. Esto resulta como consecuencia de la predisposición hacia una tipología de explotación mallada y heterogénea del sistema eléctrico. En consecuencia, en las redes inteligentes conviven dos tipos de mallas:

- ***La red eléctrica,*** la cual es la encargada del transporte de la energía.

- ***La red de datos,*** la cual asocia los paquetes de red y tramas de comunicación entre componentes, dispositivos eléctricos inteligentes y demás mecanismos de control.

En la mayoría de las instalaciones las dos redes se encuentran separadas físicamente, sin embargo, en el tramo conocido como "*la última milla*"[95] cohabitan en el mismo medio (cable) pero en distinto rango de frecuencias (energía e información).

5.5. Riesgos y amenazas existentes en las smart grids

Como se puede llegar a deducir, tras haber introducido la nueva aparición de las smart grid en la sociedad, existe un extenso abanico de sistemas y componentes diversos que conforman este nuevo paradigma.

El fundamento de la Tesis aquí presentada se basa en dos principios aplicados a la ciberseguridad los cuales se tornan imprescindibles, y que se corresponden con la creación de; *sistemas resistentes y resilientes* en IC. Estas características son trasladables directamente a las redes inteligentes para el hogar. Esto se debe a que, en los entornos de las TO, la disponibilidad y en el caso en particular de las SG, el suministro de la energía eléctrica se vuelve crítico.

Desde los orígenes de la aparición y gestión de los sistemas generadores de energía eléctrica, sus riesgos han estado asociados a la vulnerabilidad física de las instalaciones: sabotajes ocasionados por daños físicos, entradas no autorizadas, manipulado de cableado, interruptores, contadores etc., siendo muy importante su fortalecimiento físico.

Otro de los componentes clave ha sido el desconocimiento del que adolecían los propios responsables del sector, acerca de las redes eléctricas

[95] La última milla, es un término que recibe la última parte del proceso de entrega para consumo a usuario final de la energía eléctrica.

y sus redes de soporte y control, agravado esto, en muchos casos porque en diversidad de ocasiones estaban gobernadas mediante protocolos ad-hoc. Así, el factor de "seguridad por oscuridad", vuelve a aparecer en este sector.

Sin embargo, y tras la aparición de Internet, surge un nuevo modelo de gestión que hace más inteligente y autónomo a los sistemas implicados en la generación y distribución eléctrica. Los accesos pueden ser ahora recurrentes por web y la información de los sensores y actuadores se encapsula en tramas que viajan a través de protocolos de comunicación estándares como TCP/IP. Por ello, las operadoras eléctricas se ven obligadas, no únicamente a salvaguardar sus activos de amenazas físicas, sino también de posibles ataques y/o fallos lógicos o cibernéticos. Es decir, las nuevas amenazas pueden hacer uso de vectores de ataque físicos (sabotaje mediante el uso de un explosivo) o lógicos como ha sido el último referenciado en el momento de la redacción del presente capítulo "Interrupción del servicio del oleoducto de Colonial Pipeline" acaecido el 8 de mayo de 2021 [URL- 125, 2021], o incluso combinados.

Por ello, el sistema debe prepararse para garantizar una disponibilidad total y posteriormente salvaguardar la integridad del sistema y su información.

Como Anexo III, de la presente Tesis, se ha incorporado una tabla, cuyos datos se han obtenido del Instituto Nacional de Ciberseguridad, en donde se detalla a modo de resumen, los principales ciberataques perpetrados contra el sector energético en los últimos 6 años.

5.6. Protocolos GOOSE, MMS y software IEDScout

Como ya ha sido explicado al comienzo de este capítulo, el estándar de facto a desplegar en el ámbito del control eléctrico, en particular en las redes inteligentes, se corresponde con la norma IEC 61850. Este estándar asume la responsabilidad en gestión y comunicación en los sistemas de

automatización de las subestaciones (SAS). Por consiguiente, facilita que la comunicación entre los diferentes elementos de las subestaciones eléctricas se realice de forma fluida, obteniendo como resultado la interoperabilidad entre ellas.

Para que se pueda llevar de manera eficaz un control y monitorización del funcionamiento de las SAS, es preciso el intercambio de información a través de objetos orientados a los eventos de la subestación (Generic Object-Oriented Substation Event, GOOSE, por sus siglas en inglés) [Farooq S., 2019].

Dada la flexibilidad del IEC61850 y su popularidad entre las diferentes IC del sector eléctrico es trascendental tener muy en cuenta su ciberseguridad, como así ha quedado constatado por el resumen de los principales ataques sufridos en los últimos años y que ha sido indicado con anterioridad.

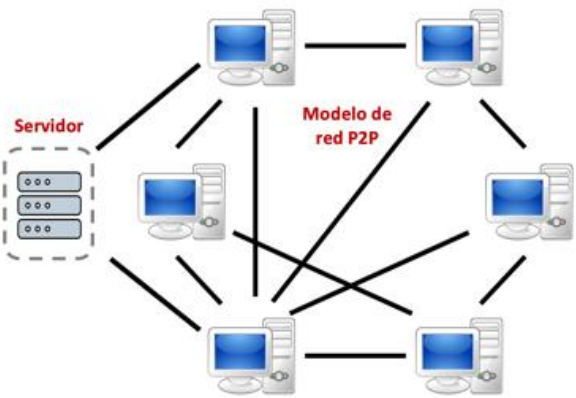


Figura 98: Modelo genérico de red P2P.

Para desplegar un sistema de comunicaciones bajo IEC61850 se hace obligatorio un conocimiento en profundidad, tanto de la las tecnologías del hardware, red, mensajería y protocolo que sustentan los servicios desplegados, siendo partícipes como actores intervinientes dentro del

modelo de comunicación peer-to-peer (p2p)[96]. La Figura 98 aclara el concepto de redes P2P.

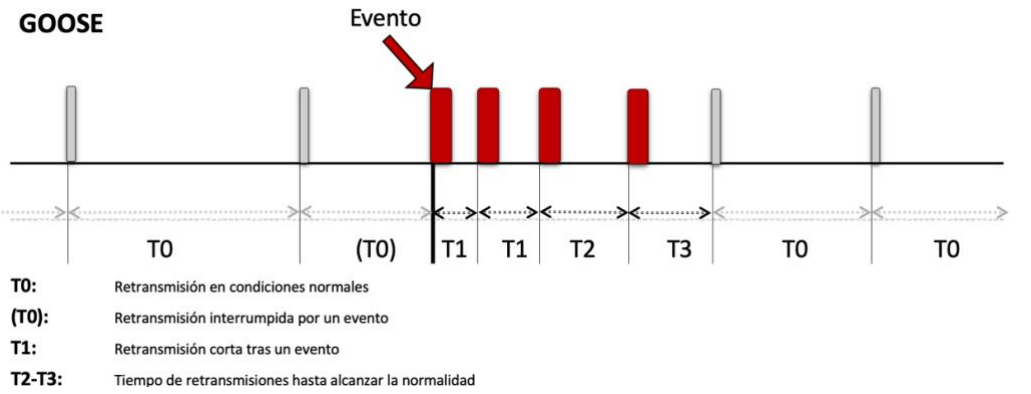


Figura 99: Escala de valores y tiempos de transmisión de los eventos (GOOSE).

La implementación de la norma IEC 61850 como estándar de comunicación, reconoce y confecciona la interacción entre dispositivos dentro de una subestación en la que se utiliza un modelo p2p para los servicios de eventos genéricos de subestación (Generic Substation Event, GSE[97] por sus siglas en inglés). Este estándar facilita una comunicación *rápida y confiable*, *que no segura*, entre los dispositivos electrónicos inteligentes (IED).

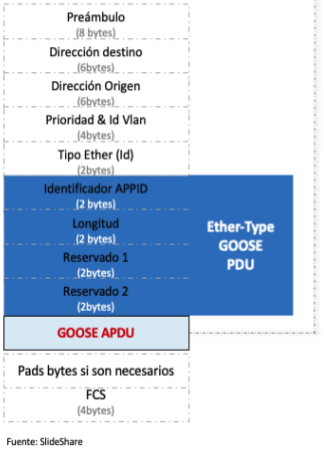
Para adquirir un diagnóstico de fallos, y el desarrollo de hardware capaz de interactuar conforme a la norma IEC61850, es imprescindible entender y poseer un conocimiento detallado de la estructura del *mensaje GOOSE*. Este conocimiento facilitó y allanó el camino para el desarrollo de las acciones llevadas a cabo en el CCDCoE, cuyo objetivo fueron el hallazgo de vulnerabilidades de los sistemas desplegados en IC del sector eléctrico.

[96] Una red *peer-to-peer*, red de pares, red entre iguales o red entre pares (*P2P*, por sus siglas en inglés) es una red de ordenadores/dispositivos en la que todos o algunos aspectos funcionan sin clientes ni servidores fijos, sino una serie de nodos que se comportan como iguales entre sí.

[97] Los eventos genéricos de subestación GSE son un modelo de control definido por la norma IEC 61850, que proporciona un mecanismo rápido y fiable de transferencia de datos y de eventos a través de redes en subestaciones eléctricas.

A través de la Figura 99, ha quedado descrita la escala de valores y el tiempo de transmisión de los eventos en GOOSE.

En la Figura 100 se describe de manera clara y concisa el formato de trama de comunicación del protocolo GOOSE el cual posee 12 campos [Farooq S., 2019]. Uno de ellos corresponde al protocolo de aplicación de la unidad de datos (Application Protocol Data Unit, APDU, por sus siglas en inglés), describiéndose los 12 parámetros que establecen la formación y envío de los mensajes.



Tag (1 byte)			
Longitud (1 o 3 bytes)			
GOOSE Pdu			
Tag (1byte)	**Longitud** (1 byte)	• **gocbRef** – (Máx 65 bytes)	Referencia única al bloque de control asociado que controla el mensaje de GOOSE
Tag	Longitud	• **timeAllowedToLive** - (Max 2bytes)	Tiempo que tiene que esperar al receptor para el próximo mensaje
Tag	Longitud	• **datSet** - (Máx 65 bytes)	Cadena que describe el nombre del *data set*
Tag	Longitud	• **goID** – (Máx 65 bytes)	Es el identificador del IED que envía el mensaje
Tag	Longitud	• **t** – (Máx 8 bytes)	Sello de tiempo que indica un nuevo evento de GOOSE
Tag	Longitud	• **stNum** - (Máx 8 bytes)	Número de veces que se ha enviado un mensaje GOOSE cuando se ha producido un cambio en los valores del *data set*
Tag	Longitud	• **sqNum** - (Máx 8 bytes)	Guarda el incremento de tiempo cada vez que un mensaje GOOSE ha sido enviado repetidamente
Tag	Longitud	• **test** – (Máx 1 byte)	Indica si el mensaje es de prueba o no
Tag	Longitud	• **confRev**- (Máx 8 bytes)	Cuenta las veces que la configuración del *data set* ha cambiado
Tag	Longitud	• **ndsCom** – (Máx 8 bytes)	Valor booleano que indica si el bloque de control requiere reconfigurarse
Tag	Longitud	• **numDataEntries** - (Máx 1 bytes)	Contiene el número de elementos que componen el conjunto de datos
Tag	Longitud	• **allData** – (Máx 65 bytes)	Datos intercambiados en el mensaje (*bool, integer, float…*). Se pueden incluir varios valores en un mismo mensaje

Figura 100: Formato de la trama de red en el protocolo GOOSE.

A través de la Figura 100 se detallan todos aquellos parámetros que identifican cada uno de los campos que parametrizan una trama de red de GOOSE. Esta trama ha sido obtenida mediante la captura del tráfico de red mediante la herramienta WireShark[98] utilizada como analizador de tráfico de red en este proyecto (ver Figura 101).

[98] WireShark es el analizador de protocolos de red más importante y utilizado del mundo.

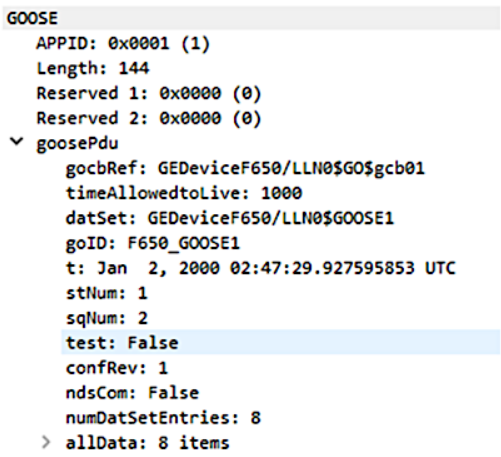


Figura 101: Captura de tráfico de red con Wireshark.

Es necesario recordar que otro de los protocolos que conforman el estándar IEC61850, se corresponde con el MMS.

De igual manera, el Script 4, definido a continuación, describe paso a paso y detalla la especificación del protocolo de aplicación para la gestión de GOOSE y GSE.

```
// NOTA: ASN.1 [99] dicta que para los parámetros cuya definición está en la
misma línea, el nombre de ese parámetro comienza con una letra minúscula.
Por lo tanto, la correspondencia de estos parámetros ASN.1 con los parámetros
de la tabla de servicios debe realizarse mediante el uso de mayúsculas en
la primera letra.

IEC61850 DEFINITIONS ::= BEGIN
IMPORTS Data FROM ISO-IEC-9506-2
IEC 61850-8-1 Specific Protocol ::= CHOICE

{ gseMngtPdu                [APPLICATION 0] IMPLICIT GSEMngtPdu,
  goosePdu                  [APPLICATION 1] IMPLICIT IECGoosePdu,
      … }
GSEMngtPdu ::= SEQUENCE
{ StateID                   [0] IMPLICIT INTEGER,
  Security                  [3] ANY OPTIONAL,
\\ reservado para una definición futura
     CHOICE
```

[99] Abstract Syntax Notation One (notación sintáctica abstracta 1, ASN.1) es una norma para representar datos independientemente de la máquina que se esté usando y sus formas de representación internas.

```
  {requests                  [1] IMPLICIT GSEMngtRequests,
  responses                  [2] IMPLICIT GSEMngtResponses
  }
 }
GSEMngtRequests ::= CHOICE
{ getGoReference             [1] IMPLICIT GetReferenceRequestPdu
  getGOOSEElementNumber      [2] IMPLICIT GetElementRequestPdu,
  getGsReference             [3] IMPLICIT GetReferenceRequestPdu,
  getGSSEDataOffset          [4] IMPLICIT GetElementRequestPdu,
…
}
GSEMngtResponses ::= CHOICE
{ gseMngtNotSupported        [0] IMPLICIT NULL,
  getGoReference             [1] IMPLICIT GSEMngtResponsePdu,
  getGOOSEElementNumber      [2] IMPLICIT GSEMngtResponsePdu,
  getGsReference             [3] IMPLICIT GSEMngtResponsePdu,
  getGSSEDataOffset          [4] IMPLICIT GSEMngtResponsePdu,
…
}
GetReferenceRequestPdu ::= SEQUENCE
{                      ident [0] IMPLICIT VISIBLE-STRING,
\\ el tamaño deberá soportar hasta 65 octetos
                      Offset [1] IMPLICIT SEQUENCE OF INTEGER,
…}
GetElementRequestPdu   ::= SEQUENCE
{                      ident [0] IMPLICIT VISIBLE-STRING,
\\ el tamaño deberá soportar hasta 65 octetos
                 references [1] IMPLICIT SEQUENCE OF VISIBLE-STRING,
…
}
GSEMngtResponsePdu ::= SEQUENCE
{                      ident [0] IMPLICIT VISIBLE-STRING,
\\ respuestas del valor de la solicitud
                     confRev [1] IMPLICIT INTEGER OPTIONAL,CHOICE
{responsePositive            [2] IMPLICIT SEQUENCE {
datSet                       [0] IMPLICIT VISIBLE_STRING OPTIONAL,
result                       [1] IMPLICIT SEQUENCE OF RequestResults
},
responseNegative             [3] IMPLICIT GlbErrors
},
…
}
RequestResults::= CHOICE
{                       offset [0] IMPLICIT INTEGER,
                    reference [1] IMPLICIT IA5STRING,
                        error [2] IMPLICIT ErrorReason
}
GlbErrors ::= INTEGER
{                            other(0),
             unknownControlBlock(1),
                responseTooLarge(2),
```

```
controlBlockConfigurationError (3),
…
}
ErrorReason ::= INTEGER
{
                          other (0),
                       notFound (1),
…
}
IECGoosePdu ::= SEQUENCE
{                    gocbRef [0] IMPLICIT VISIBLE-STRING,
           timeAllowedtoLive [1] IMPLICIT INTEGER,
                      datSet [2] IMPLICIT VISIBLE-STRING,
                        goID [3] IMPLICIT VISIBLE-STRING OPTIONAL,
                           t [4] IMPLICIT UtcTime,
                       stNum [5] IMPLICIT INTEGER,
                       sqNum [6] IMPLICIT INTEGER,
                        test [7] IMPLICIT BOOLEAN DEFAULT FALSE,
                     confRev [8] IMPLICIT INTEGER,
                      ndsCom [9] IMPLICIT BOOLEAN DEFAULT FALSE,
           numDatSetEntries [10] IMPLICIT INTEGER,
                    allData [11] IMPLICIT SEQUENCE OF Data,
                   security [12] ANY OPTIONAL,
\\ reservado para la firma digital
}
UtcTime:: = OCTETSTRING
\\Formato y tamaño definido en el apartado 8.1.3.6. del International Standar
IEC 61850
END
```

Script 4: IEC 61850-8-1, especificación del protocolo (modificado de la fuente original: IEC).

La definición al completo del protocolo y de las especificaciones aquí representadas se encuentran ubicadas en el repositorio de documentación habilitado al efecto para la presente *Tesis* [URL- 00, 2020].

Los sistemas de automatización de subestaciones eléctricas basados en la norma IEC 61850, emplean principalmente los protocolos GOOSE y MMS. Dado que los mensajes GOOSE y MMS carecen de seguridad de cifrado en su transmisión, esto incide directamente en la aparición de un vector de debilidad ante su posible vulneración. Un ciber-atacante podría observar la información de la cabecera de los paquetes en los mensajes del protocolo y variar ciertos mensajes pudiendo llevar a cabo acciones y/o ataques en un sistema de automatización de subestaciones. Estas acciones se pueden llegar

a materializarse inclusive, mediante software debidamente licenciado y utilizado específicamente para la gestión y monitorización de dichas comunicaciones realizadas entre los IED y los sistemas SCADA.

Para que pueda concretarse la comprobación del envío de este tipo de paquetes de red en la comunicación, es ineludible tener acceso al tráfico de la red del segmento correspondiente de la subestación.

La interacción entre cliente/servidor (IED- SCADA) habitualmente consiste en secuencias de petición/respuesta. La tecnología utilizada para esta comunicación se define en la norma IEC 61850-8-1 así como la especificación del tipo de mensajería MMS.

La Figura 102, detalla la composición y valores correspondientes a un objeto tipificado e identificado por la norma IEC-61850-8-1.

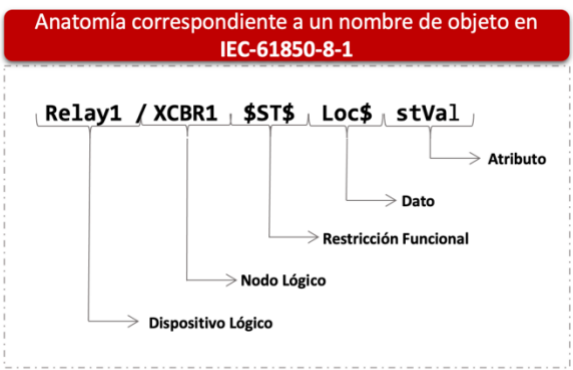


Figura 102: Anatomía correspondiente un nombre de objeto en IEC-61850-8-1.

En IEC 61850-8-1, se detalla la metodología para convertir la información proveniente del modelo en un objeto variable (MMS) asociándole un nombre, el cual da como resultado una referencia única e inequívoca para cada uno de los elementos de datos del modelo [Mackiewicz, R., 2006].

Por otro lado, y para la intervención y realización de las acciones especificadas en este capítulo, ha sido indispensable la utilización de IEDScout[100] [URL- 139, 2021].

IEDScout se corresponde con un cliente de carácter universal para IED de subestación eléctrica con protocolo de comunicación orquestado a través del estándar IEC 61850. Este software es utilizado como editor/suscriptor de mensajes GOOSE. A su vez, IEDScout proporciona varias funciones de subestación, desde la lectura/escritura de atributos de datos hasta el uso de la función de auto-descripción de un IED y la producción de archivos de información y configuración estandarizada (Substation Configuration Language, SCL por sus siglas en inglés).

Para poder ejecutar la detección de los IED se requiere de un conocimiento previo de la configuración de la red Ethernet entre los IED, siendo importante conocer las direcciones IP individuales de cada IED [Hadbah, A., 2014].

A través de la Figura 103, correspondiente a una captura de pantalla de la máquina virtual en donde se encuentra desplegado el software de control, se puede observar la pantalla principal del IEDScout. En ella se muestran las zonas principales del panel de navegación dentro del propio software.

[100] IEDScout es una herramienta que permite el acceso a los IED (dispositivos electrónicos inteligentes) ideal para técnicos de automatización de protección y de subestaciones que trabajan con dispositivos IEC 61850.

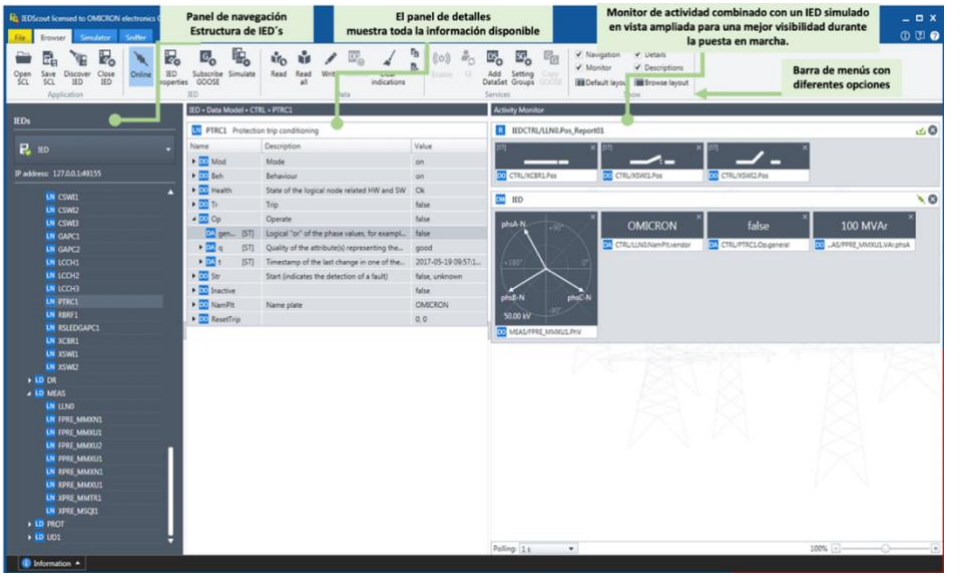


Figura 103: Pantalla principal de IEDScout V.5.

En el repositorio de documentación habilitado para la presente Tesis se encuentra la documentación completa del software IEDScout V. 5.0 [URL-00, 2020].

5.6.1. Debilidades del protocolo GOOSE

Una de las principales características que potencia la debilidad del protocolo GOOSE se encuentra íntimamente ligada con la exigua tolerancia a la latencia en las comunicaciones. Ésta es la principal barrera que emerge a la hora de implementar medidas de seguridad, especialmente en infraestructuras del sistema eléctrico, donde la celeridad es un elemento clave para poder maniobrar de forma eficaz.

La implementación técnica del protocolo GOOSE establece ***4 ms*** como tiempo máximo de desfase para determinados mensajes, por lo que las medidas de seguridad a aplicar, como las expuestas en la IEC 62351, deben cumplir con este requisito. Como consecuencia directa de estos requerimientos, las medidas de cifrado o cualquier otra que aumente el desfase o la latencia están excluidas.

INCIBE-CERT, en su blog de ciberseguridad, posee una entrada denominada “Control de peticiones multidifusión en el estándar IEC 61850” [URL- 137, 2021], por la que esclarece que según el propio estándar, es necesario llevar a cabo la entrega de paquetes de comunicación de los dispositivos en la red, en un plazo comprendido entre **2 y 10 ms.** El estándar IEC 62351-6 [URL- 138, 2021], confía en la autenticación de los mensajes de GOOSE mediante firmas de clave públicas, aunque no se puede garantizar los requisitos de latencia derivadas de las comprobaciones de firmas. Como se puede deducir, una mínima alteración en los ínfimos plazos de latencia podría conllevar una disrupción del servicio.

Como posible solución a esta problemática y para conseguir un cifrado de los datos en un intervalo de tiempo dentro de los márgenes permitidos, sería necesario poseer una CPU de gran potencia instalada en los IED. Esto, a corto y medio plazo, puede suponer un problema, ya que, al introducir una nueva CPU, es necesario un rediseño del hardware y, en la mayoría de las ocasiones, eso conllevaría la necesidad de certificar el nuevo diseño.

En la actualidad se están implementado mejoras sustanciales en los tiempos de cifrado, motivando estos una mejora de la ciberseguridad en cuanto a comunicaciones cifradas se refiere [Kriger C., 2013], [Reda H., 2021], [Lahza H., 2017], [Farooq S., 2019].

5.7. Caso de estudio y análisis desarrollados en la investigación llevada a cabo en el CCDCoE

El contenido del presente apartado muestra los datos observados tras la realización de un estudio pormenorizado de la arquitectura de red, así como los datos que discurrían por esa arquitectura mediante la utilización de diferente software de auditoría y gestión. Las acciones llevadas a cabo

remarcan y corroboran ciertas carencias importantes en este sector desde el punto de vista de la ciberseguridad.

Los componentes de hardware implicados y necesarios para el despliegue conciernen a un total de 24 IED correspondientes a 10 fabricantes diferentes (SIEMENS, ABB, SCHNEIDER ELECTRIC, ARCTEQ, Toshiba, Woodward, Schweitzer, General Electric, Basler e ICE).

A su vez ha sido necesaria la creación de una matriz de 24 terminales remotos de la serie SICAM A8000 del fabricante SIEMENS, los cuales se encontraban operados por sus respectivos sistemas SCADA. La serie A8000 de SICAM representa una nueva generación de dispositivos modulares los cuales aportan soluciones sobre aplicaciones para el telecontrol y automatización en todos los ámbitos del suministro de energía eléctrica.

De igual manera, se hizo necesario la utilización de un software específico instalado en diferentes máquinas virtuales que facilitó la obtención de los resultados que se detallarán a continuación. Este software se corresponde con una distribución del SO de auditoría *Kali Linux,* del analizador de red *WireShark* y del software de gestión y telecontrol *IEDScout* 5.0.

El trabajo se inició mediante la revisión de todos y cada uno de los parámetros, objetos, modelos y servicios implementados en cada uno de los IED existentes y desplegados en las tres cabinas de mando (a modo de laboratorio de pruebas), y en paralelo conectados con sus respectivos SICAM A8000.

Estos tres armarios de operación y sus componentes se muestran en la Figura 104, la cual representa la arquitectura desplegada en el CCDCoE.

Los resultados logrados, y que se exponen a continuación, no son los correspondientes a la evaluación del total de los IED existentes. Se muestran solo los hechos que conforman el núcleo verdaderamente importante de la

investigación, y que han permitido comprobar y verificar vulnerabilidades y carencias existentes en las comunicaciones, así como en la seguridad de la red en la que se encuentra el IED conectado con su respectivo SICAM.

5.8. Procedimiento, arquitectura e instrumentación del banco de pruebas utilizado en la investigación

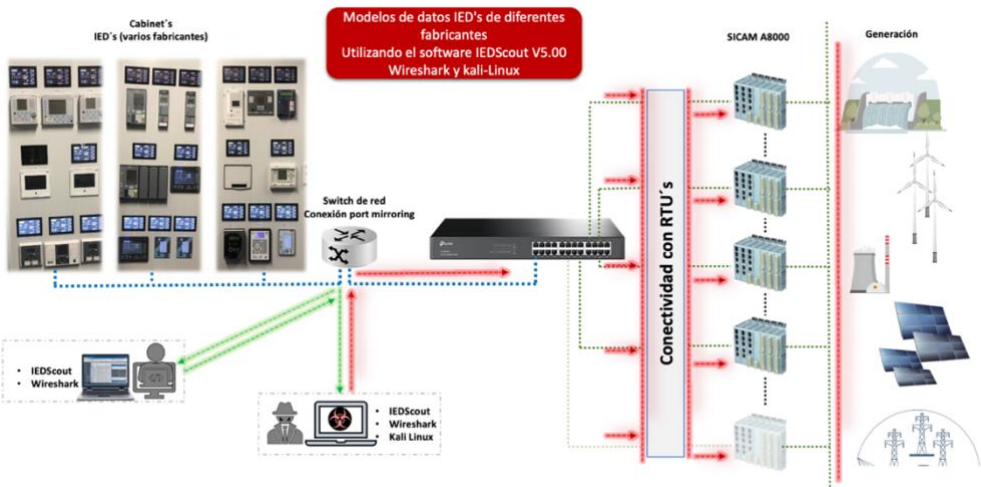


Figura 104: Esquema de la arquitectura desplegada para la investigación en el CCDCoE.

El análisis de red se realizó a través de una máquina virtual de VmWare (VMware Fusion 11.5). Esta máquina corresponde con un sistema Windows 7 (Professional x64), que tiene instalado el software IEDScout V.5. y un analizador de tráfico de red WireShark.

La forma de materializar el enlace se realizó directamente mediante cable RJ-45, configurando la dirección IP de la máquina virtual dentro del mismo rango del IED (10.x.5.100) en el adaptador del host de VmWare, realizando la traducción de direcciones de red, también llamado enmascaramiento del direccionamiento IP (Network Address Translation, NAT, por sus siglas en inglés) a través del adaptador.

El esquema de conectividad, que se muestra en la Figura 104, detalla el escenario desarrollado. El objetivo fue poder llevar a cabo el análisis del

tráfico de red existente en los diferentes anillos de la infraestructura de generación y transporte energético (IRD, RTU, SCADA, generación).

Es de suma importancia destacar que para analizar el tráfico del protocolo MMS, al conectarse IEDScout a cualquiera de los IED es primordial que para tener la capacidad de previsualización del software IEDScout, el equipo donde se encuentre desplegado WireShark esté conectado a través del interruptor de red mediante un puerto configurado como espejo ("port mirroring"[101]) del rúter. Si no se hace así, WireShark tiene problemas para realizar la disección del tráfico, identificándolo con el protocolo de presentación del modelo OSI (*PRES*[102]*),* no pudiendo ser totalmente comprensibles los octetos capturados. Este protocolo está definido en la norma ISO 8823 y en la recomendación UIT-T X.226, formando parte de la *IsoProtocolFamily* [URL- 140, 2021].

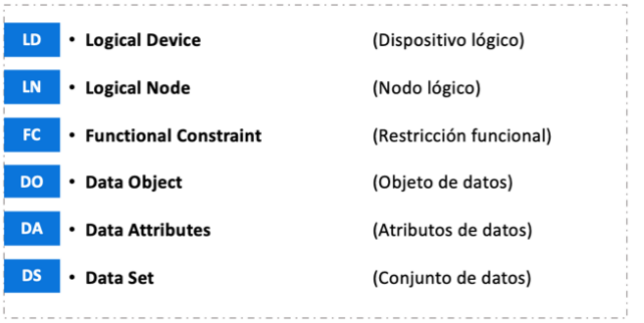


Figura 105: Iconos y nomenclatura frecuente de IEDScout.

Para ayudar a comprender la nomenclatura de IEDScout, la Figura 105 especifica la simbología representada y empleada por el software de ingeniería para el fin buscado en este capítulo. Las especificaciones al completo de todos y cada uno de los parámetros se encuentran en el

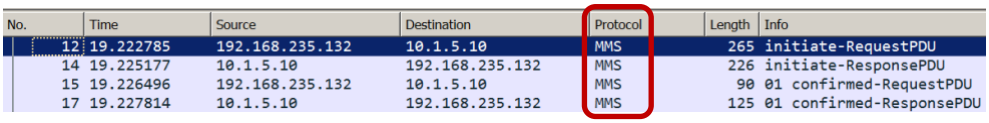
[101] El puerto espejo o port mirroring es utilizado con un switch de red para enviar copias de paquetes de red vistos en un puerto del switch (o una VLAN entera) a una conexión de red monitoreada en otro puerto del switch.

[102] Este protocolo se define como la norma ISO 8823 y la recomendación UIT-T X.226.

repositorio de documentación habilitado para la presente Tesis bajo el nombre *"IEDScout_v5_manual.pdf "* [URL- 00, 2020].

Para representar gráficamente lo explicado anteriormente se muestran dos imágenes obtenidas de las conexiones realizadas inicialmente.

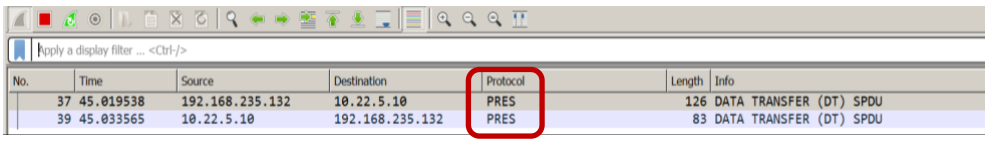
- La primera (la Figura 106) habiendo arrancado el WireShark antes de la conexión con el IEDScout.



No.	Time	Source	Destination	Protocol	Length	Info
12	19.222785	192.168.235.132	10.1.5.10	MMS	265	initiate-RequestPDU
14	19.225177	10.1.5.10	192.168.235.132	MMS	226	initiate-ResponsePDU
15	19.226496	192.168.235.132	10.1.5.10	MMS	90	01 confirmed-RequestPDU
17	19.227814	10.1.5.10	192.168.235.132	MMS	125	01 confirmed-ResponsePDU

Figura 106: Captura de red con wireshark, previa a la conexión contra el IEDScout.

- La Figura 107 muestra la acción contraria, materialización de la conexión contra el IED previamente a la inicialización del wireshark.



No.	Time	Source	Destination	Protocol	Length	Info
37	45.019538	192.168.235.132	10.22.5.10	PRES	126	DATA TRANSFER (DT) SPDU
39	45.033565	10.22.5.10	192.168.235.132	PRES	83	DATA TRANSFER (DT) SPDU

Figura 107: Captura de red con wireshark, a posteriori a la conexión contra el IEDScout

Para la presentación y análisis de los datos obtenidos de los diferentes dispositivos electrónicos sometidos a estudio, la fuente principal de datos ha sido centralizada a través del panel de navegación de configuraciones de los IED "Estructura IED´s" mediante su conexión física a través del switch de red (port mirroring) del software IEDScout. En la Figura 108, a través del panel de navegación y estructura del IED, contra el que se ha realizado la conexión y resaltada por un recuadro de color rojo, se indica la sección correspondiente en el software de ingeniería, en donde se muestran los datos de configuración y conexión desde IEDScout al IED.

La Figura 109, particulariza las características concretas que se evaluaron en cada uno de los IED´s que fueron utilizados para la investigación ejecutada.

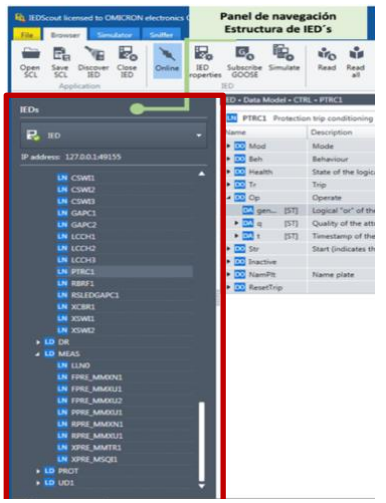


Figura 109: Datos de configuración de IED, mostrados por el software de ingeniería.

- ***GOOSE*** (Protocolo)
- ***Reports.*** (Informes)
- ***Setting groups.*** (Configuración de grupos)
- ***Files.*** (Archivos)
- ***Data sets.*** (Conjunto de datos)
- ***Data model*** (Modelo de datos)

Figura 108: Relación de características evaluadas en BT01_IED y BT15_I.

Sobre el trabajo llevado a cabo, a continuación se presentan y analizan los datos obtenidos mediante el software y hardware descrito en apartados anteriores, correspondientes a dos IED diferentes y de fabricantes distintos.

5.9. Análisis de los datos del IED del fabricante ABB

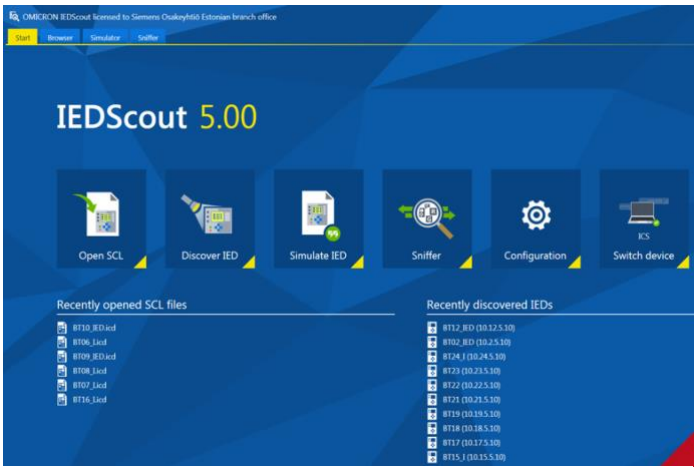


Figura 110: Pantalla principal IEDScout.

Al proceder a inicializar el software de gestión e ingeniería IEDScout (ver Figura 110) el cual se halla desplegado en la máquina virtual conectada según la arquitectura de red descrita previamente, se disponen de ciertas posibilidades de actuación/configuración para ser ejecutadas en la conexión que se quieran efectuar. Estas variedades se corresponden con:

1. Mediante la apertura de un fichero *.icd*[103] *(IED Configuration Description).* Este archivo se corresponde con un fichero de configuración de un dispositivo concreto, previamente configurado a través de IEDScout. En el Script 5, se muestra parte del contenido de un fichero .icd, el cual corresponde con uno de los IED utilizados para el presente estudio, en concreto con el *BT15_I*. El fichero completo se encuentra disponible en el repositorio de documentación habilitado [URL-00, 2021].
2. Mediante la realización y ejecución de un descubrimiento en la red de los elementos (IED) conectados en el mismo rango.
3. Mediante la simulación de un dispositivo, lo cual arroja capacidades importantes desde el punto de vista de la ciberseguridad, otorgando

[103] Fichero de descripción y configuración válido para los IED.

capacidades preventivas al entorno. Proporciona diversas opciones de configuración y facilita un analizador propio de tráfico de red.

```
\\ El contenido de este fichero xml se corresponde con parte del fichero
de configuración del IED BT15_I
      <?xml version="1.0" encoding="UTF-8"?>
      <!--Created by ekukk with OMICRON IEDScout 4.20 licensed to Empower,
Estonia-->
      <!--SCL Schema Version 1.6 (2013/08/14)-->
      <SCLxmlns="http://www.iec.ch/61850/2003/SCL"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.iec.ch/61850/2003/SCL SCL.xsd">
            <Header id="" version="" revision="" toolID="OMICRON IEDScout"
nameStructure="IEDName" />
            <Communication>
                  <SubNetwork name="NONE" type="8-MMS">
                        <ConnectedAP iedName="BT15_I" apName="P1">
                  <Address>
                        <P type="IP" xsi:type="tP_IP">10.15.5.10</P>
                        <P type="OSI-TSEL" xsi:type="tP_OSI-TSEL">0001</P>
                        <P type="OSI-SSEL" xsi:type="tP_OSI-SSEL">0001</P>
                        <P type="OSI-PSEL" xsi:type="tP_OSI-
PSEL">00000001</P>
                        <P type="OSI-AP-Title">1,1,1,999,1</P>
                        <P type="OSI-AP-Invoke" xsi:type="tP_OSI-AP-
Invoke">0</P>
                        <P type="OSI-AE-Qualifier" xsi:type="tP_OSI-AE-
Qualifier">12</P>
                        <P type="OSI-AE-Invoke" xsi:type="tP_OSI-AE-
Invoke">0</P>
                  </Address>
            <GSE ldInst="EDRelay" cbName="GSE_CB1">
            <Address>
                  <P type="MAC-Address" xsi:type="tP_MAC-Address">01-0C-
CD-01-00-0F</P>
                  <P type="APPID" xsi:type="tP_APPID">0000</P>
                  <P type="VLAN-ID" xsi:type="tP_VLAN-ID">000</P>
                  <P type="VLAN-PRIORITY" xsi:type="tP_VLAN-
PRIORITY">4</P>
            </Address>
                  </GSE>
                  </ConnectedAP>
                  </SubNetwork>
            </Communication>
<IED name="BT15_I">
                  <Services>
                        <DynAssociation />
                        <GetDirectory />
                        <GetDataObjectDefinition />
                        <DataObjectDirectory />
                        <GetDataSetValue />
                        <SetDataSetValue />
                        <DataSetDirectory />
                        <ConfDataSet max="3" modify="false" />
                        <DynDataSet max="42" />
                        <ReadWrite />
                        <ConfReportControl max="8" />
                        <GetCBValues />
                        <ReportSettings rptID="Dyn" optFields="Dyn"
bufTime="Dyn" trgOps="Dyn" intgPd="Dyn" />
                        <ConfLNs fixPrefix="true" fixLnInst="true" />
                        <GOOSE max="1" />
                        <GSSE max="0" />
                        <FileHandling />
                  </Services>
            <AccessPoint name="P1">
```

```
            <Server>
                  <Authentication none="true" />
                  <LDevice inst="EDRelay">
                  <LN0 lnType="BT15_IEDRelay.LLN0" lnClass="LLN0" inst="">
                  <DataSet name="DataSetGOOSE1">
                                                <FCDA ldInst="EDRelay"
prefix="LO" lnClass="GGIO" lnInst="1" doName="Ind1" fc="ST" />
                                                <FCDA ldInst="EDRelay"
prefix="LO" lnClass="GGIO" lnInst="1" doName="Ind2" fc="ST" />
                                                <FCDA ldInst="EDRelay"
prefix="LO" lnClass="GGIO" lnInst="1" doName="Ind3" fc="ST" />
                                                <FCDA ldInst="EDRelay"
prefix="LO" lnClass="GGIO" lnInst="1" doName="Ind4" fc="ST" />
                                                <FCDA ldInst="EDRelay"
prefix="LO" lnClass="GGIO" lnInst="1" doName="Ind5" fc="ST" />
                                                <FCDA ldInst="EDRelay"
prefix="LO" lnClass="GGIO" lnInst="1" doName="Ind6" fc="ST" />

</DataSet>
```

Script 5: Archivo XML de configuración correspondiente al IED BT15_I.

Este último sólo ha sido considerado, para el caso de estudio que nos ocupa, es decir, para la verificación de tráfico de red punto a punto entre el IED y el IEDScout, habiendo sido clave la operatividad del servicio de WireShark levantado en una máquina con capacidad operacional para un despliegue tipo "*man in the middle*" [URL- 141, 2020], como queda representado en la Figura 111.

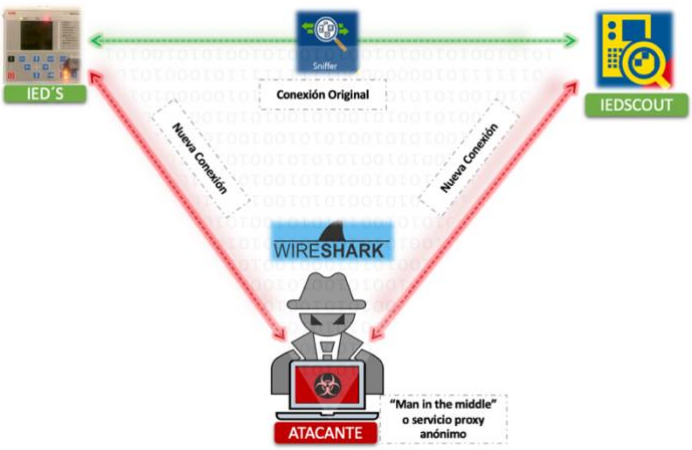


Figura 111: Representación gráfica de posible acción del tipo "man in the middle" recreada en el caso de investigación llevada a cabo.

El primer IED utilizado para el análisis de posibles vulnerabilidades es el correspondiente a la marca ABB.

Figura 112: Conexión establecida contra el BT01_IED.

ABB es una corporación tecnológica multinacional con sede en Zúrich, Suiza, especializada en robótica, generación de energía eléctrica, automatización, equipamientos industriales y otras tecnologías de ingeniería [URL- 142, 2021].

Al comenzar con sus configuraciones, tras proceder a su inicialización, si se habilita en "Propiedades del IED" (Contraseña), en el momento de establecer la conexión online, el sistema solicita la contraseña: si se introduce algún carácter, el sistema *"permite la conexión online".*; por el contrario si en el momento de cumplimentar la contraseña, sin introducir ningún carácter se pulsa "aceptar", el sistema se pone en línea de manera automática. Como se puede comprobar en la Figura 112 se muestra el icono de conexión en verde (parte superior), lo que indica que la conexión contra el IED se ha producido con éxito.

- **GOOSE**

Después de hacer los cambios en los parámetros en las "*propiedades del IED*", y así forzar la autenticación mediante contraseña, cuando se lleva a cabo la conexión contra el IED a través de IEDScout, los caracteres que se introducen en el cuadro de texto requerido para la autenticación, son los correspondientes a las credenciales solicitadas para la correcta autenticación. Esta pertenece a la contraseña de identificación.

Para corroborar estos datos utilizando la arquitectura de red y conexión detallada en la Figura 98 (correspondiente a la conexión general),

se hizo preciso el despliegue de un analizador de red independiente del proporcionado por IEDScout. Este caso fue WireShark.

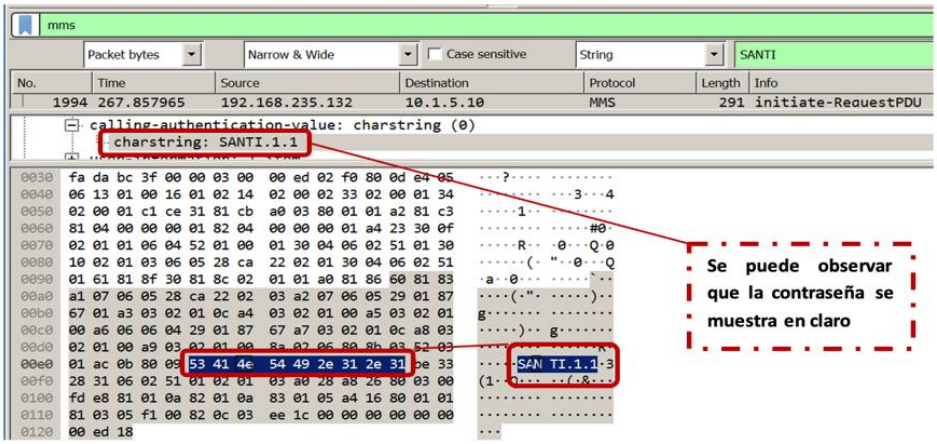


Figura 113: Captura de tráfico de red con wireshark, contraseña en claro.

Los resultados obtenidos tras una búsqueda minuciosa entre los paquetes de red generados y capturados mediante la conexión se pueden observar en la Figura 113. Los resultados desvelan la existencia del campo de texto introducido en el IED, como credenciales de identificación; el texto ***"SANTI.1.1"***, se puede visualizar directamente en las tramas capturadas en la red.

- **Reports**

Los informes facilitados por el dispositivo electrónico inteligente analizado no cuentan con una significación relevante para el estudio llevado a cabo. Sólo mencionar uno calificado como destacable, que es el correspondiente al de *protección del sistema*, el cual no es modificable en tiempo real.

La Figura 114 muestra el historial del estado del IED con el que se ha establecido la conexión, indicando la descripción del suceso, el código asociado y el horario registrado.

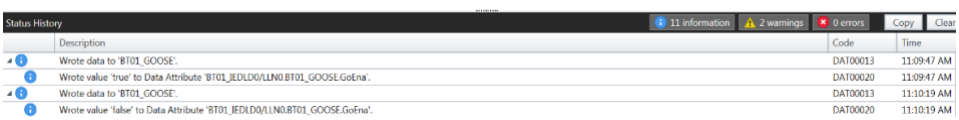


Figura 114: Historial de estado del IED (Reports).

- **Setting Groups**

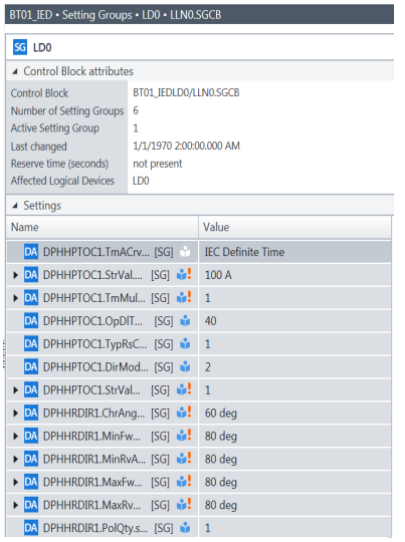


Figura 115: Bloque de atributos del IED (Setting groups).

A través de este grupo de opciones se dispone de un conjunto de ajustes correspondientes al bloque del control de atributos, que a su vez son configurables a través de la conexión pero no en "caliente", es decir, no es posible su modificación en tiempo real. Es necesario interrumpir la conexión, cambiar los parámetros y volver a cargarlos en el dispositivo. La Figura 115 relaciona el bloque de atributos facilitado por el software de ingeniería.

- **Files**

En este apartado, y de forma común a todos los fabricantes testeados para el caso de estudio, se dispone de una gran cantidad de archivos que pueden ser descargados para su posterior análisis. La Figura 116 muestra el contenido de uno de ellos, en concreto los correspondientes a la configuración básica del IED.

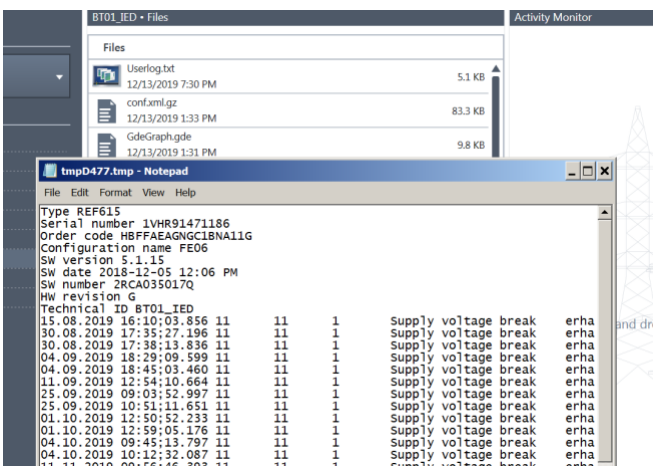


Figura 116: Relación de ficheros del IED (Files).

- **Data Sets**

La norma 61850 utiliza el concepto de conjuntos de datos (data sets) para representar una colección de particularidades de ciertas características. Un conjunto de características con sus respectivos atributos [Hadbah, A., 2014].

- **Data Model**

La norma IEC 61850, a su vez, contiene modelos de mecanismos que describen las propiedades y la asignación de funciones en un dispositivo físico. Proporciona modelos de datos orientados a objetos que definen servicios genéricos para el intercambio de mensajes cliente/servidor entre los dispositivos de una subestación y para la transferencia de todo tipo de informes, respetando las estrictas restricciones de la transmisión, como la velocidad, la fiabilidad y la seguridad [Ustun T., 2013].

Como ha sido descrito previamente, el software de ingeniería utilizado permite la realización en tiempo real de ciertas acciones. Una de las más peligrosas y críticas es el poder cambiar el estado de los relés. El relé de tensión manejado en concreto por el dispositivo conectado a IEDScout, se corresponde con un interruptor de protección multifuncional y versátil diseñado para la protección de sobre y sub-tensiones, y está dedicado a supervisar redes de distribución de media tensión.

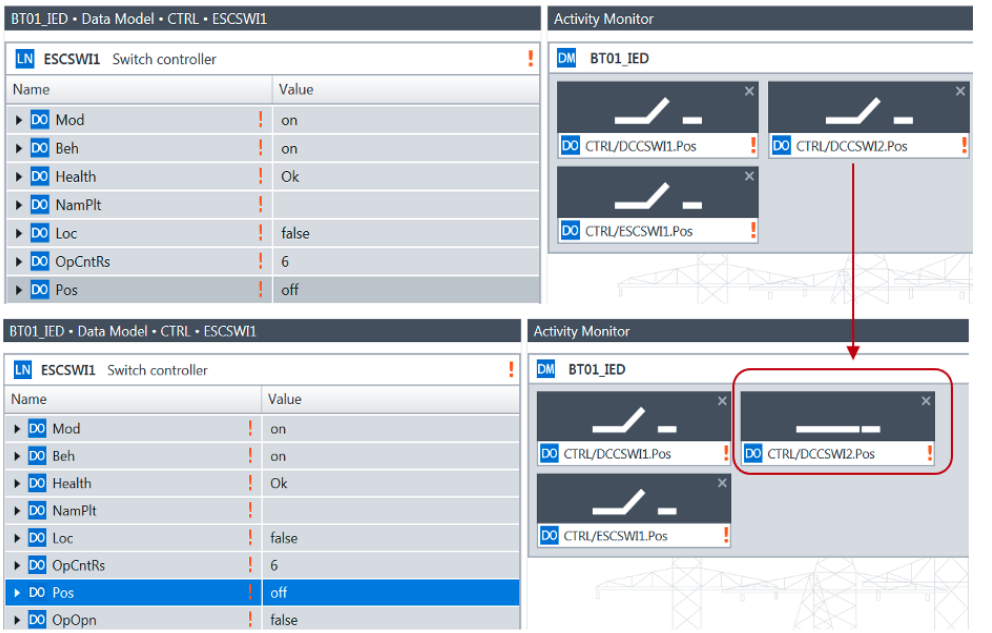


Figura 117: Información a referente a modelos de datos en BT01_IED (Data model).

Este dispositivo también se puede usar para proteger generadores, transformadores y motores de diferente funcionalidad. Al realizar cambios en los relés desde el panel *"Monitor de actividad"* con el botón *"Control",* se manipularán los estados de los relés. La Figura 117*,* obtenida del software de ingeniería, muestra gráficamente el estado y posicionamiento de los relés configurados en el IED accedido.

5.9.1. Análisis de los datos del IED del fabricante ARCTEQ

El segundo IED utilizado para el análisis de posibles vulnerabilidades es el correspondiente a la marca ARCTEQ. ARCTEQ son los pioneros en la protección contra el arco eléctrico[104], y son conocidos por fabricar los relés de protección más precisos del mundo. Su sede y las instalaciones de fabricación se encuentran en Vaasa, Finlandia.

[104] En electricidad se denomina arco eléctrico o también arco voltaico a la descarga eléctrica que se forma entre dos electrodos sometidos a una diferencia de potencial y colocados en el seno de una atmósfera gaseosa.

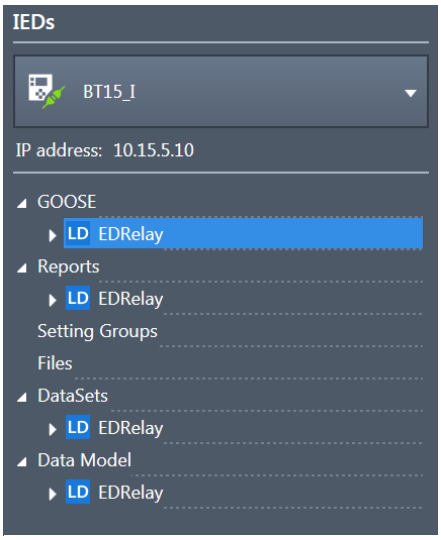


Figura 118: Conexión establecida con BT15_I.

Durante la última década, los productos de ARCTEQ se han ido desplegando a lo largo de todos los continentes. Además de poseer un compromiso con la alta calidad en sus productos, atesoran un compromiso para la mejora de la ingeniería eléctrica en la industria, proporcionando apoyo y servicios para su obtención [URL- 143, 2021]. La conexión contra este dispositivo fue realizada mediante el establecimiento de un canal de comunicación con la máquina virtual a través de un switch y uno de sus puertos de comunicación, configurado éste último como puerto espejo, procediendo a levantar una instancia de WireShark desde el host para obtener el tráfico GOOSE y MMS entre IED y IEDScout. La Figura 118 confirma la conexión establecida con el IED denominado BT15.

De igual manera que en el anterior dispositivo, se pasan a detallar los parámetros relevantes dentro de los siguientes apartados (Figura 119).

- **GOOSE**

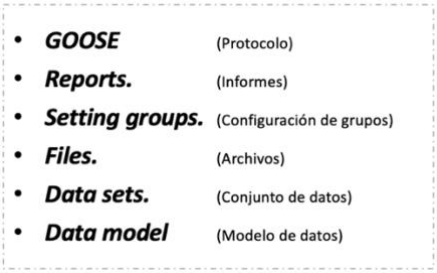


Figura 119: Relación de características evaluadas en BT01_IED y BT15_I (II).

Inmediatamente después de hacer los cambios pertinentes en los parámetros de las propiedades del IED para proceder a forzar la autenticación con el dispositivo mediante la utilización de contraseña, al establecerse la conexión entre el IED y el IEDScout, los caracteres que se

introduce en el cuadro de texto mostrado por la aplicación, corresponden con la contraseña solicitada para la identificación.

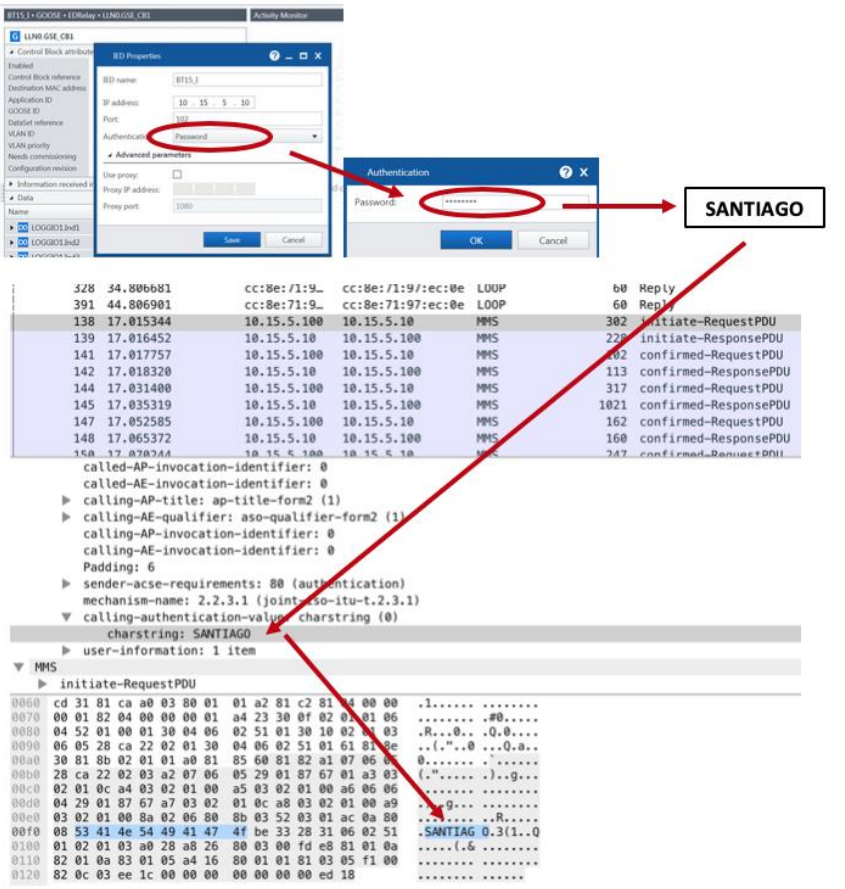


Figura 120: Captura de tráfico a través de wireshark (contraseña en claro BT15_I).

Según se muestra en la Figura 120 mediante un análisis exhaustivo de las tramas de red capturadas por WireShark, levantado como servicio en un host independiente de la red corporativa de la infraestructura se obtienen datos concluyentes que demuestran que la contraseña viaja sin encriptar y puede ser copiada.

A través de esa acción se pone de manifiesto la peligrosidad de este tipo de conexiones en estas infraestructuras.

- **Reports, setting groups and files**

Los parámetros detectados y configurables en este IED en concreto revelan la misma variabilidad que los de otros dispositivos electrónicos inteligentes sometidos a estudio, no ofreciendo datos relevantes a la investigación

- **Data sets**

Figura 121: Información a referente al conjunto de datos (Data set).

En este apartado se muestra, que tras haber realizado diversos cambios en el ***DataSet LD EDRelay LLN=.DataSetGOOSE1-URCB1*** presente en la Figura 121, como parte del software de ingeniería, se presentan diversos mensajes de error. Estos son arrojados por la necesidad de reiniciar la conexión con el IED y su nuevo rearme ante un cambio sustancial.

- **Data model**

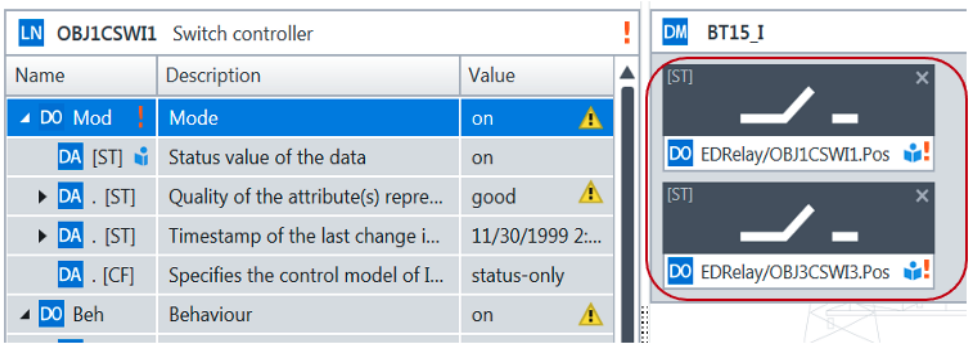


Figura 122: Cambios de estado de los relés, registrados por IEDScout.

Dentro de los modelos de datos manejados, existen una variedad muy amplia de ellos. Los que se muestran a continuación, corresponden con uno de los más importantes por las consecuencias de sus acciones y tratamiento de manera inapropiada. Destaca el que permite cambiar los valores de los diferentes relés de protección eléctrica. Los relés han cambiado su valor de "***CERRADO*** a ***ABIERTO***" (ver Figura 122).

DA ctlM... [CF]	Specifies the control model of IEC 61850...	status-only
◢ DO NamPlt !	Name plate	Arcteq Relays *SIEMENS(
DA ven... [DC]	Name of the vendor	Arcteq Relays *SIEMENS(
DA swRev [DC]	SW-revision	CHANGED
DA d [DC]	Textual description of the data	CHANGED ID

Figura 123: Cambios en los atributos registrados por IEDScout.

Como se observa en las Figuras 122 y 123 los atributos (Data attributes, DA) han sido modificados, observándose esta situación en concreto en la Figura 123 y a través de la captura de tráfico de red realizada con Wireshark plasmada en la Figura 124.

Estos datos son importantes porque pueden generar confusión a la hora de la identificación remota de los elementos desplegados, pudiendo generar errores en el momento de materializar actualizaciones de firmware, cargar configuraciones etc.

```
    284  23.656267      10.17.5.100           10.17.5.10            PRES          157  DATA TRANSFER (DT) SPDU
▶ Frame 284: 157 bytes on wire (1256 bits), 157 bytes captured (1256 bits) on interface 0
▶ Ethernet II, Src: Apple_d0:3d:06 (68:5b:35:d0:3d:06), Dst: Toshiba_00:79:fd (ec:21:e5:00:79:fd)
▶ Internet Protocol Version 4, Src: 10.17.5.100, Dst: 10.17.5.10
▶ Transmission Control Protocol, Src Port: 51232 (51232), Dst Port: 102 (102), Seq: 2370, Ack: 898, Len: 103
▶ TPKT, Version: 3, Length: 103
▶ ISO 8073/X.224 COTP Connection-Oriented Transport Protocol
0000  ec 21 e5 00 79 fd 68 5b  35 d0 3d 06 08 00 45 00   .!..y.h[ 5.=...E.
0010  00 8f 00 00 40 00 40 06  00 00 0a 11 05 64 0a 11   ....@.@. .....d..
0020  05 0a c8 20 00 66 8b 8a  20 a9 00 01 8f 96 50 18   ... .f.. .....P.
0030  ff ff 1f 11 00 00 03 00  00 67 02 f0 80 01 00 01   ........ .g......
0040  00 61 5a 30 58 02 01 03  a0 53 a0 51 02 02 03 25   .aZ0X... .S.Q...%
0050  a4 4b 80 01 00 a1 46 a0  44 30 22 a0 20 a1 1e 1a   .K....F. D0". ...
0060  08 42 54 31 37 43 74 72  6c 1a 12 43 53 57 49 31   .BT17Ctr l..CSWI1
0070  24 53 54 24 50 6f 73 24  73 74 56 61 6c 30 1e a0   $ST$Pos$ stVal0..
0080  1c a1 1a 1a 08 42 54 31  37 43 74 72 6c 1a 0e 43   .....BT1 7Ctrl..C
0090  53 57 49 31 24 53 54 24  50 6f 73 24 71            SWI1$ST$ Pos$q
```

Figura 124: Captura de tráfico de red de origen IED, destino nodo maestro.

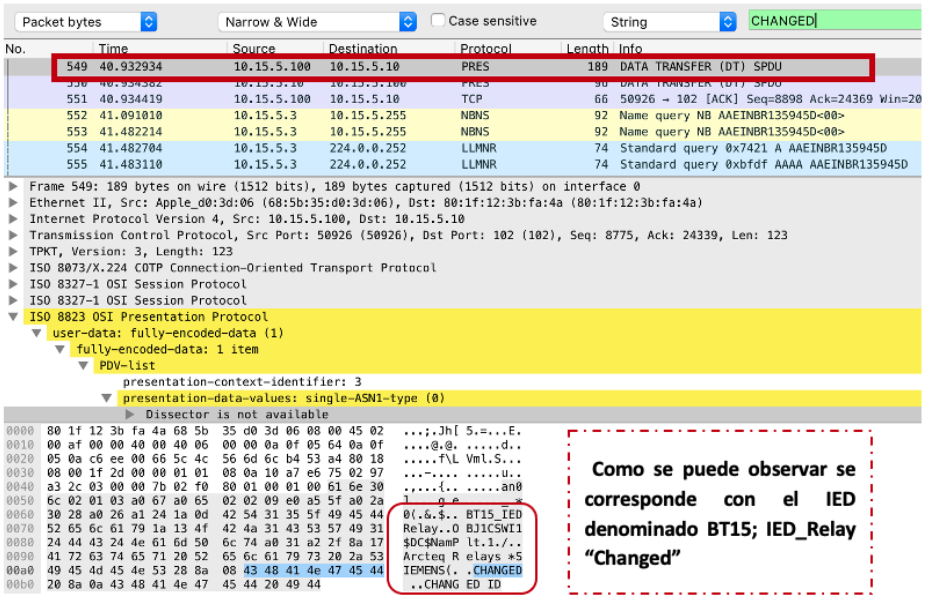


Figura 125: Captura de tráfico de red mediante wireshark (tráfico en claro).

La Figura 125 ha sido obtenida a través del WireShark conectado desde una línea exterior a la de producción, volviendo a corroborar que los datos de configuraciones, estado, acciones y definiciones de los relés, viajan sin cifrar por la red. Por consiguiente, se puede crear un script que modifique estas capacidades para, posteriormente, inyectar en la red paquetes con intencionalidad maliciosa.

Como consecuencia de otro modelo de datos analizado, se muestran en la Figura 125, los datos transmitidos de manera constante desde el IED hacia el nodo configurado como maestro en la red, por el que se informa del estado del circuito y que han sido capturados a través de WireShark. Los datos transmitidos constantemente desde la *IP 10.17.5.100* hacia la *IP 10.17.5.10* en ***CSWI1STPos$stVal0*** corresponden al estado de "circuito abierto" como se puede comprobar a través de la Figura 126.

En la Figura 127, se muestra otra captura de tráfico de red, identificando la nomenclatura del relay (***ItemId: CGI01TMod%stVal***) cuyo estado puede ser modificado.

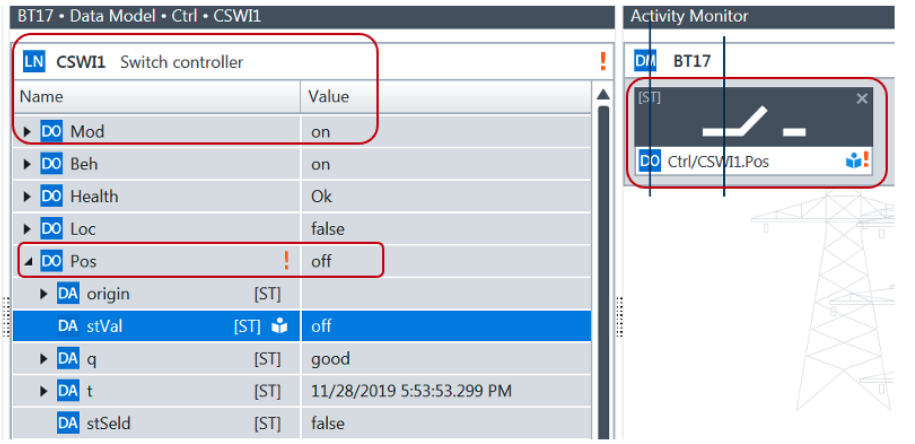


Figura 127: Data model Circuito "abierto".

En la Figura 127, se muestra otra captura de tráfico de red, identificando la nomenclatura del relay (***ItemId: CGI01TMod%stVal***) cuyo estado puede ser modificado.

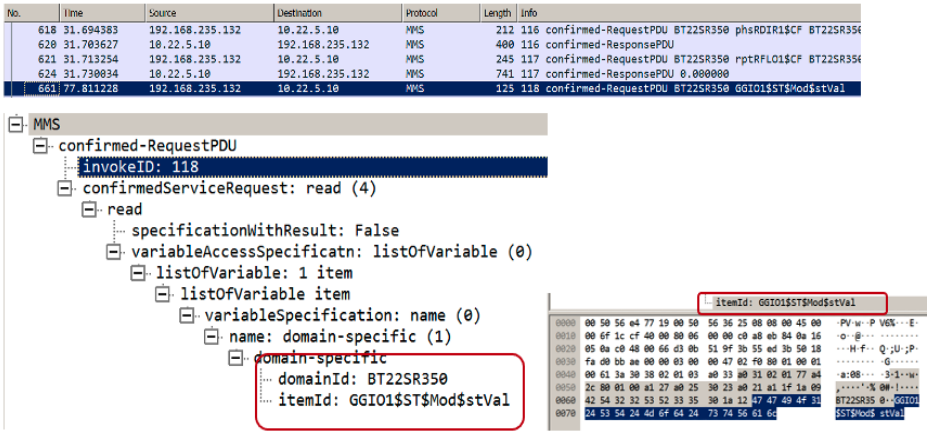


Figura 126: Identificación del Item Id: **(CGI01TMod%stVal)** a través de captura de paquetes de red mediante wireshark.

El *DS LLN0. DataSetBRCB1* contiene los controladores de los interruptores de los tres relés. Como se puede ver en la primera imagen de la Figura 126, el estado de los relés se corresponde con el estado abierto, ***"off"***.

Con la opción "Control" se modifica el estado de los relés, pasándolos a la posición ***"on"*** e incluso se puede variar la opción "*Originator Category*", pudiendo así enmascarar el origen del cambio.

El tráfico de WireShark correspondiente a todos estos cambios y ficheros mostrados se encuentran almacenados en el repositorio de documentación habilitado al efecto para esta Tesis Doctoral (carpeta: *C-01-Ficheros_.pcap snifer de red*) [URL- 00, 2020].

5.10. Resultados y conclusiones alcanzadas del estudio llevado a cabo con los IED, ABB y ARCTEQ

Tras las pruebas realizadas y mostradas en este capítulo, la acción analizada que destaca entra todas las demás se corresponde con la forma de proceder para proteger el protocolo de comunicación GOOSE. Desde que unos investigadores de seguridad demostraron que el protocolo GOOSE podía ser comprometido mediante diferentes ciberataques, se evidenció la necesidad de aplicar mecanismos de defensa que asegurasen la integridad de este protocolo [Miranda J., 2014].

Los ataques que se podían llevar a cabo sobre este protocolo estaban basados en:

- ***Modificación del tráfico*:** Capturando paquetes y modificando algunos parámetros se podría provocar el encendido de alertas en los interruptores de la subestación.
- ***Denegación del servicio (DoS):*** Enviando más paquetes que el número de paquetes permitido en un intervalo de tiempo, consiguiendo que el IED atacado no respondiese a las peticiones.

Esta investigación ha estado focalizada en las posibilidades de modificación del tráfico de red existente y la corroboración de esta situación en infraestructuras reales a día de hoy, por lo que se puede verificar que se siguen manteniendo en el tiempo estas carencias. Sí es cierto que las tecnologías han mejorado sus características reactivas ante disrupciones sobrevenidas en los servicios, pero sigue existiendo una enorme carencia de

protección de los que se puede considerar el pilar base, correspondiendo con la forma de proteger el protocolo GOOSE y MMS.

5.11. Resumen

En este capítulo han sido llevadas a cabo acciones de investigación sobre un área muy específica como es el transporte y consumo de la energía eléctrica. Este sector posee muchas connotaciones que le otorgan una naturaleza muy especial. La energía eléctrica es el pilar fundamental desde donde se sustenta la civilización y el desarrollo del ser humano tal y como hoy en día lo concebimos. Por este motivo se ha dedicado un capítulo íntegro al mismo.

En primer lugar, y tras haber introducido la importancia de los hechos aquí presentados, surge un nuevo concepto no visto hasta el momento, pero que va a llevar el peso y la justificación de los análisis efectuados. Este es el concepto de redes inteligentes o smart grid.

Seguidamente, se argumentaron las premisas que justifican el porqué debe jugar un papel clave la protección cibernética de los sistemas y automatismos involucrados dentro de las smart grid, y de los sistemas que controlan, gestionan y transportan la energía eléctrica hasta su punto de consumo. Esta subsección vino a ser reforzada a través de un detallado procedimiento, en donde quedaron reflejados todos los elementos intervinientes, así como la arquitectura desplegada al efecto.

Consecutivamente, y con el fin de obtener el punto de partida de las pruebas a las que fueron sometidos los entornos desplegados para su evaluación, han sido detallados, exhaustivamente los protocolos de comunicación involucrados en estos escenarios. A su vez, corresponde una mención especial al hecho de la aparición de nuevos riesgos y amenazas como resultado del cambio de paradigma experimentado, consecuencia éste de la transición habida entre un enfoque puramente “eléctrico” hacia un

enfoque “eléctrico + gestión y control de datos” en el área de la generación y transporte de la energía.

Después de obtener las características técnicas y los requisitos operacionales del sistema a evaluar en su conjunto y, en particular, los protocolos de comunicación al uso, y habiendo llevado a cabo un planteamiento previo de las potenciales problemáticas asociadas al entorno en concreto, se centraron los esfuerzos en la búsqueda de vulnerabilidades de las comunicaciones entre dispositivos en el marco de las arquitecturas y estándares desplegados en las smart grid.

Finalmente, se han mostrado todos aquellos parámetros y debilidades que han destacado en el seno de esta investigación, centrados principalmente en aquellos que, de una manera intencionada o no, fruto de su perturbación redundaría en consecuencias altamente peligrosas para el entorno, los sistemas e incluso las vidas humanas.

Para la obtención de los datos aquí presentados han sido necesarios elementos reales de infraestructuras eléctricas, así como software altamente especializado en el sector. Todos estos elementos son propiedad del Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN sito en Tallin (Estonia) (NATO Cooperative Cyber Defence Centre of Excellence, CCDCoE).

Capítulo VI

Conclusiones y líneas futuras.

6. Preámbulo

El punto de partida de esta investigación se fijó en la definición conceptual de los modelos de los sistemas de control industrial y de su situación originaria, la cual se correspondía con un despliegue completamente aislado de cualquier ambiente colaborativo. Estos entornos en su origen fueron concebidos para una disponibilidad incorruptible, sin tener en cuenta los conceptos de integridad y confidencialidad en los datos requeridos ni proporcionados como consecuencia y necesidad de su funcionamiento.

Progresivamente, y como resultado de la aparición de nuevos y diversos elementos energéticos para su uso, del aprovechamiento en la automatización y de las nuevas formas de llevar a cabo los procesos en la industria se han ido produciendo cambios relevantes en estos sistemas, dando lugar a las diversas revoluciones industriales.

Ya en la época actual y como consecuencia del aporte tecnológico de las TI a la operativa de las TO se encuentra definido un nuevo paradigma directamente relacionado con la era de la interconexión, en la cual, nos encontramos involucrados actualmente. Dada esta vertiginosa adaptabilidad y afinidad, afloran nuevas amenazas a las que se encuentran expuestos los SACI y, por ende, las infraestructuras críticas. Es por lo que se debe potenciar las capacidades preventivas de estos entornos para así evitar las disrupciones, intencionadas o no, de estas IC, puesto que de lo contrario, se asume un riesgo grave en todos aquellos parámetros implicados como criterios horizontales de criticidad definidos en la Ley 8/2011 de PIC.

La verdadera versatilidad del sistema aquí presentado viene dada por la alta adaptabilidad para la incorporación de tantas CAI como fabricantes de sistemas de control industrial y automatismos existen. A su vez, el hecho de proporcionar todo el software involucrado en estas redes permite aumentar la calidad del análisis de la vulnerabilidad. En consecuencia, la principal aportación de esta investigación, materializada mediante SICERCAI, es la provisión de un marco seguro que ayudará a obtener un análisis que demuestre el verdadero estado de madurez de una arquitectura industrial que los usuarios podrían desplegar en función de sus necesidades de investigación o desarrollo.

6.1. Conclusiones

Una vez examinados y evaluados los resultados obtenidos, las principales conclusiones del trabajo de investigación realizado han sido:

1) En este trabajo se ha presentado el desarrollo de un nuevo concepto de simulación de procesos en entornos industriales mediante el aprendizaje por experimentación real, aprovechando los avances en el mundo de las TI. En la actualidad, con el aumento de la presencia de las TI en el ámbito del control y de la automatización, los sistemas industriales se están viendo expuestos a un gran número de nuevas ciber-amenazas. Teniendo en cuenta el importante papel que juegan las infraestructuras y servicios esenciales para el normal desarrollo y convivencia de la sociedad, se debe considerar que la tendencia de los ciberataques, tanto actuales como futuras, pasarán por los intentos de violación de la integridad de estas instalaciones [Genge B., 2015].

2) Ha quedado demostrado que retoma un valor trascendental el descartar la idea de que la "seguridad por desconocimiento" se correspondería con un método válido de protección contra este tipo de ataques. Por ello, es muy importante estar preparado para posibles

eventualidades mediante "prácticas y pruebas" [Stergiopoulss G., 2015], obteniendo así un alto grado de resiliencia [Roldán G., 2017], [Chaves A., 2017], [González S., -2020]. Al mismo tiempo queda resaltada la importancia de poder obtener un alto nivel de madurez y anticipación ante los nuevos vectores que darán acceso a los ciberataques en los sistemas de control industrial, siendo la mejor defensa ante estos nuevos retos; la formación, familiarización y experimentación previa en entornos controlados.

3) A su vez, es destacable la aplicación de los conocimientos teóricos sin asumir el riesgo que supone la puesta en práctica de estos análisis en las plantas de producción, fomentando estos entornos la experimentación y análisis previo a las implantaciones. Todas estas capacidades prácticas han sido puestas de manifiesto en esta Tesis empleando SICERCAI a través del uso y evaluación de un entorno vulnerable, encontrándose esta debilidad debidamente documentada y cuyo impacto era relevante desde el punto de vista de la ciberseguridad.

4) Mediante la aplicabilidad de SICERCAI en el laboratorio se ha verificado la eficacia de las capacidades preventivas y reactivas, quedando completamente neutralizada la peligrosidad de la vulnerabilidad elegida como prueba de concepto para el presente estudio de investigación.

5) De igual manera, en el capítulo correspondiente a la búsqueda de vulnerabilidades en ciertos componentes y en los estándares involucrados en las etapas de generación y transporte de la energía eléctrica, se han aportado hechos relevantes para la investigación. Este sector posee muchas connotaciones que le confieren una naturaleza muy especial ya que la energía eléctrica constituye el pilar esencial en

donde se sustentan los SACI partícipes en las IC. El sector eléctrico en general, y las smart grid en particular, vienen a justificar el papel clave que la protección cibernética debe jugar dentro de los sistemas y automatismos involucrados en estas infraestructuras. El hecho de la aparición de nuevos riesgos y amenazas como resultado del cambio de paradigma experimentado, consecuencia éste de la transición habida entre un enfoque puramente "eléctrico" dirigido a hacia un enfoque "eléctrico + gestión y control de datos", en el área de la generación y transporte de la energía, viene a evidenciar este tipo de evaluaciones. Mediante la utilización de un entorno real creado al efecto fueron llevados a cabo test de valoración y diseño con las correspondientes evaluaciones en ciberseguridad. Se centraron los esfuerzos en la búsqueda de vulnerabilidades de las comunicaciones entre dispositivos en el marco de las arquitecturas y estándares desplegados en las smart grid. Como resultado fue corroborada la existencia de diferentes brechas de seguridad de naturaleza crítica, tanto en dispositivos de hardware desplegado, como en los estándares de comunicación, software propietario de ingeniería y gestión, y diseños de los despliegues y sus configuraciones.

6.2. Líneas futuras de investigación

Esta subsección establece el punto de partida para aquellas acciones que han quedado identificadas como posibles puntos de continuidad de esta investigación. Estas líneas futuras han sido encuadradas dentro de dos áreas: las asociadas a SICERCAI y las que están relacionadas con su aplicación en el sector eléctrico.

6.2.1. SICERCAI

Las futuras líneas de investigación en materia de prevención y resiliencia en ciberseguridad en entornos y SACI detallados en esta Tesis pasan por:

- La incorporación y creación de nuevas CAI de diferentes fabricantes. De esta manera se alcanzaría una heterogeneidad en componentes que garantizarían una aproximación real a la arquitectura de la industria existente.
- Adhesión de SICERCAI a organizaciones más complejas de carácter híbrido respecto a los fabricantes industriales, como puede ser la Red Nacional de Laboratorios Industriales (RNLI[105]) para aumentar el potencial de evaluación de arquitecturas industriales.
- Incorporación de la taxonomía de los ciberataques (Cyber Attack Taxonomy, CAT por sus siglas en inglés) [Intelligence-Led, 2019], como modelo de análisis y representación de los ciberataques a recrear por SICERCAI. El modelo estratégico del CAT ayudará a simplificar la comprensión y el diseño de los ciberataques, estandarizará la interpretación de la forma en que operan los actores, permitirá reproducir fielmente las acciones llevadas a cabo por los atacantes y descartará soluciones como la aplicabilidad de contramedidas "*instintivas sin testar*". Así pues, la funcionalidad establecida en CAT encaja perfectamente con la base fundamental de la creación de SICERCAI, que es recrear y verificar los SACI, plasmando y documentando debidamente todas y cada una de las fases en las siete capas de los modelos de detección del nivel de madurez [Mavroeidis V., 2017], y permaneciendo completamente

[105] La Red Nacional de Laboratorios Industriales es una plataforma de laboratorios industriales con capacidad de experimentar e investigar soluciones que aumenten los niveles de seguridad de las infraestructuras industriales nacionales.

alineado con las recomendaciones de la Comisión Europea, fruto de la incipiente inquietud de fomentar la creación de entidades certificadoras en ciberseguridad industrial y por extensión a la CTIO.

- El impulso de este tipo de arquitecturas para fijar criterios orientados a la estandarización de un marco de certificación de los componentes de los SACI en el área de la ciberseguridad a nivel europeo, afectando por extensión a sus infraestructuras críticas.
- La evaluación del diseño de los protocolos de comunicación en la industria para obtener así una optimización de las comunicaciones entre los controladores lógicos programables incorporados a SICERCAI.
- La potenciación de la investigación para la incorporación de tecnologías Blockchain[106] para la mejora de la problemática sobre autenticación, comunicación y disponibilidad en los SACI.

6.2.2. SACI involucrados en generación y transporte eléctrico

De igual manera las futuras líneas de investigación en esta área de investigación pasarían por:

- La potenciación de la recreación de laboratorios de pruebas híbridos (fabricantes, y arquitecturas) para una aproximación al mundo real desplegado en las smart grid.
- Adhesión y obtención de capacidades de acceso a los propios laboratorios de los principales fabricantes de los terminales remotos utilizados en el sector.
- Investigación de la potenciación de las medidas de seguridad en los protocolos y estándares implicados en las comunicaciones, focalizando los esfuerzos en la parte de no interferencia entre sistemas de cifrado en los

[106] Se corresponde con una estructura de datos cuya información se agrupa y viaja en forma de bloques, en los cuales se aplican técnicas criptográficas para su protección, consiguiendo un histórico irrefutable de la información portada.

canales de comunicación y la baja tolerancia en tiempos de latencia requeridos por las infraestructuras del sector.

- Trabajo en profundidad a cerca de las medidas a llevar a cabo para una potenciación y optimización de la unidades centrales de proceso de los diversos RTU, en pro de la mejora de los tiempos de latencia en las comunicaciones industriales debido a la incorporación de sistemas de cifrado en las mismas.
- Evaluación en profundidad de los protocolos GOOSE y MMS en su estructura de trama de red para la obtención de mejoras en las comunicaciones, todas ellas encaminadas a la potenciación de niveles de confianza en las comunicaciones cifradas extremo a extremo.
- La realización de un estudio que permita instaurar una metodología de entrenamiento eficaz con el cual se puedan elegir las mejores muestras para formar un sólido punto de partida hacia el cambio y/o adaptabilidad en un protocolo nuevo de comunicaciones más seguro que los analizados en esta Tesis.
- La ejecución de un estudio pormenorizado que proporcione capacidades de prevención ante posibles acciones disruptivas en el sector eléctrico (áreas de generación y transportes) mediante la aplicabilidad de técnica de inteligencia artificial para la industria.

Capítulo VII

7. Introduction

Throughout history, human beings have been building machines that facilitate their work where great physical efforts were required, or a risky exposure of their safety and integrity, thus achieving an increase in productivity and efficiency. The vast majority of authors/researchers agree that the first machine invented by humans was the wheel. The authors estimate that it was invented in the fifth millennium BC in Mesopotamia during the period of El Obeid (4500 bC) [URL- 01, 2021] in the ancient region known as Fertile Crescent, initially with the potter's wheel function. It was later used in the construction of chariots, expanding throughout the Old World along with wagons and dray animals. It is usually believed that the wheel migrated to Europe and Western Asia in the fourth millennium bC, and to the culture of the Indo Valley around the third millennium bC. However, the oldest known wagon wheel was found in Slovenia.

Barbieri-Baja (2000) defends the existence of vehicles of eastern origin (China) which had wheels were dated around 2000 bC, although its oldest reference dates from around 1200 bC.

Among American cultures it did not prosper, probably because of the absence of large animals that could pull wagons, and because the most advanced civilizations occupied steep and difficult to access terrain. Wheels have been found on Olmec objects identified as toys dating back to around 1500 bC. Later, they were used in the construction of carts. [URL- 02, 2008].

These devices were increasing in mechanical complexity, such as levers, pulleys, straps or cogwheels, transforming the movements of the different parts of the machine to achieve the desired action.

These changes defined a framework in which processes of technological, economic, social and political evolution were being involved. The transformations that took place were so profound that no similar change had been seen in the world since the Neolithic revolution, which occurred some 10,000 years earlier, when it moved from rural and agrarian societies and economies to urban and industrial ones.[107]

The real milestone that marked a qualitative leap in the definition of "industry", and that today we associate with this definition, was the emergence of energy sources for the automation of processes (water-vapor, electricity, oil), as well as the technification of industry in the XXI century, providing interconnectivity and interoperability[108] to processes at a global level.

Following the logical evolution of the contemporary concept of industry, it can be considered that it begins to gain strength at the end of the eighteenth century, being unstoppable this day. In this sense, four major industrial revolutions are considered:

- *The first industrial revolution,* dated 1784, occurs with the appearance of mechanical production equipment powered by water and energy from water vapor. Its introduction into the printing press transformed the

107 The Neolithic Revolution is the first radical transformation of the way of life of humanity, which went from nomadic OT sedentary, when a productive economy based on agriculture and livestock was realized. This expression is due to Vere Gordon Childe.

108 According to the Royal Spanish Academy, technify, in its first meaning is defined as the "introduction of modern technical procedures in industries that did not use them". In its second meaning it is defined as "making something more efficient from the technological point of view".

medium into the primary communication tool. The definition of "Industry 1.0" arises.

- *The second industrial revolution,* dated in the nineteenth century and more specifically in 1870, occurs with the emergence of electricity and oil as energy sources for mass production. The concept of the production chain and the division of the work to be carried out in more elementary tasks arises. The definition of "Industry 2.0" appears.
- *The third industrial* revolution, scientific-technical revolution or intelligence revolution, dated 1970, occurs with the use of components based on electronic systems and information technologies in their production systems. This movement is characterized, in turn, by five main peculiarities:
    a) Use of renewable energies such as hydro, solar or wind energy.
    b) Innovations in energy storage media and processes, such as the use of rechargeable batteries or hydrogen batteries.
    c) The impulse of the smart grid or "smart grid" electric power distribution network [Sarker E., 2021].
    d) The development of electric vehicle-based transport (all electric vehicles, plug-in hybrids and non-plug-in electric hybrids) as well as the technological progress of fuel cells, using renewable electricity as propulsion energy. The appearance of electrical energy as a method of propulsion, propitiates the beginning of the era "Industry 3.0."
- *The fourth industrial* revolution, dated in 2011, originates with the emergence of cybernetic physical systems for automated and interconnected production. This implies the promise of a new revolution that combines advanced production and operations techniques with

intelligent technologies that will be integrated into organizations, people and assets. The definition of "Industry 4.0" arises.

Finally, and as a clarification, automation is postulated as a key piece to differentiate the current stage, the 4th revolution, from the 3rd industrial revolution. With maximum connectivity and extreme computing power, automation will be critical changing the industrial era.

Coming to give greater clarity, machines in Industry 4.0 work autonomously without the intervention of a human being, while in Industry 3.0 machines were only automated.[109]

This revolution is marked by the emergence of new technologies such as robotics, analytics, artificial intelligence, cognitive technologies, nanotechnology and the Internet of Things, coming to add electronic mechanisms and sensors to the devices, and thus increasing their technological and functional capabilities. The main purpose pursued with this type of complements is the collection of data, its analysis and the materialization of large-scale automated actions. When applied to industry it can be called “the industrial Internet of Things”.

Today, the 4th industrial revolution is in full swing. This is because today's emerging intercommunication and connectivity mark the starting point of its development. It is worth noting regarding connectivity, that there are already more than 7 billion mobile devices connected to hundreds of millions of people [URL- 03, 2020]. In turn, there are also more than 22,000 million devices (or machines) connected through the Internet (cars, telephones, homes, machinery, airplanes, trucks, boats, soft drink machines, etc.) In addition, with the arrival and implementation of 5G technology there

[109]According to the Royal Spanish Academy, automating is "*applying the automatic OT a process or a device*".

will be more devices that can be connected to the different systems. It is expected that by the year 2025 the number of devices connected to the Internet will exceed 38,000 million [URL- 04, 2020].

7.1. Information Technologies and Operating Technologies

As detailed in the previous section, the irruption and evolution of the different industrial revolutions has led to the emergence of new technologies in each of them. Thus, it can be observed how since the first industrial revolution in which machines are created by combining mechanical elements to save efforts (pulleys, gears, etc.) together with propulsion elements (water vapor), society has evolved towards the 4th industrial revolution, where the use of communications and computing technologies is enhanced, using network communication and state-of-the-art protocols, such as 5G intercom networks[110].

As a result of this differentiation due to its specialization, the concepts defined as Information Technologies (IT[111]) and Operating Technologies (OT[112]) arise. They can be considered and defined as different but not exclusive concepts. Before delving into the definition of these two concepts, there are several basic aspects that are mentioned below and that come to emphasize the main differentiating characteristics existing between them:

- *Technologies*

[110] 5G implies a new generation of communication networks that come to combine an increase in speed, lower latency, much greater flexibility in device management and a considerably lower consumption by this technology.

[111] Information technologies (IT) are the application of computers and telecommunications equipment to store, retrieve, transmit and manipulate data, often used in the context of business or other companies.

[112] The areas that performs the management of devices, networks and applications related to the monitoring and control of industrial processes are the so-called Operation Technologies (OT).

One of the main differences corresponds to the predominant technology itself in each environment. While in the industrial area are specified and can speak of sensors, controllers, actuators, conveyor belts, mechanics etc., on the IT side [URL- 05, 2015] it talks about database environments, document managers, directories of credentials and permissions, web and mail servers, etc. For these reasons, the knowledge that the profiles-users of each technology have is completely different and supposes a great distance between them.

Similarly, the needs demanded by each of the technologies are not comparable. In the IT area, it is observed that the needs are associated with a management and delegation environment, where the number of assets does not differ too much with the number of users. However, if we talk about the OT environment, we have a multitude of devices spread over a wide and scattered space, in most cases, and their association for administration and management demands considerably fewer people in proportion to IT.

It is important to emphasize that the production environments associated with OT inherently have associated extreme operating conditions (temperature, voltage, humidity, radiation, etc.), nothing comparable to IT environments.

- *Security perspective*

  OT correspond to technologies and means that facilitate work where interaction with machines and electromechanical devices is prevalent. The importance of hazard exemption, from the point of view of physical and process safety (safety), is paramount. When talking about safety, the definition is focusing on the protection of the environment, people and infrastructures against possible failures in the process. In IT systems, by not putting lives at risk, it refers to a security from the logical point of view

(security[113]), that is, to protect the information with respect to any type of risk that may endanger it, whether it is people, natural disasters, instrumental deterioration, etc. Both types of security seek to protect the confidentiality, integrity, and availability of system information in their environments [Morante N., 2019]. But both areas understand security from different approaches and, in turn, pursue their security objectives unevenly. In production environments, the critical aspect to protect is availability, since an unexpected stop in production (due to monetary losses, possible natural and human disasters, etc.) is not permissible. While in IT, the confidentiality of information and security in data are the priority aspects.

- *Software-Hardware-Operating Systems*

  Industrial control systems are dominated by special purpose computers with proprietary operating systems, unlike the IT world where standard operating systems predominate, mostly systems based on Windows architectures[114], as well as a lot of commercial software installed on each computer to meet the needs of workers (databases, word processors, office software, etc.) If a detailed study is carried out in the area of communications, in the same way, there are in the production environments proprietary protocols of the manufacturers of industrial elements (S7, OPC, Modbus, Profibus, etc.)[115]; while in information technologies, for the main tasks that are performed, you can find

[113] *Security* is the term coined for security related OT risks of antisocial origin, that is, intentionally caused by people to cause harm to other people, property, etc.

[114] In 1985, Microsoft released the first version of Windows, a graphical user interface (GUI) for its own operating system (MS-DOS) that had been included in the IBM PC and supported since 1981.

[115] The industrial communication protocol is composed of a set of rules that allow interference and data exchanges between several devices that form a network.

protocols associated with navigation and web interconnection, that is, HTTP / HTTPS over TCP / IP[116].

- *Frequency of updates*

  There is a big difference between the update rates of IT and OT systems. The IT area, given its high profile of technological variability, has a nature that becomes vulnerable and, therefore, demands updates on a permanent basis. As these are more dynamic environments, it is easy to find these errors and solve them. However, OT systems, due to their original nature of invariability and physical and technological isolation, must remain in operation for long periods of time, so they cannot be patched frequently, as this would require a reboot or situations of downtime of systems not acceptable in production environments. If these systems are deactivated, then all production processes would be stopped with all the economic losses and possible risks of different natures that this would entail. This lack of updates directly impacts on the fact that, all too often in OT environments, obsolete and highly vulnerable controllers, actuators, sensors, etc. are deployed.

7.2. Convergence of Information Technologies and Operating Technologies

Once the main differences between IT and OT have been clarified in the previous section, it is necessary to specify them again to make clear the convergence between both technologies, and thus highlight the importance

[116] Group of network protocols that make it possible to transfer data over networks, between computers and the Internet.

of both within the 4th industrial revolution. While the technologies used in OT are very popular for operators and engineers working in the sector, their knowledge is limited for IT staff. Traditionally, IT and OT environments have been treated separately and in isolation, with no interdependencies between them. The existing distance has shown that the information exchanged between these environments has not been adequate, and the important benefits of concurrency, such as understanding security risks and increasing performance, demand greater attention at all levels. The operation of a multitude of industries, especially those encompassed in the strategic/critical sectors of a country, such as energy, transport, water, chemical, research, space, communications, etc., are increasingly dependent on communications and computer networks.

Below, and as a summary, there is a table in which it is possible to compare the classifications carried out by different countries, where the strategic sectors and their web reference to the managing body are specified (Table 27), [URL- 06, 2016].

Country	Strategic/critical infrastructure sectors	Organism	Reference
Spain	**12 Strategic Sectors:** • *Administration* • *Space* • *Nuclear industry* • *Chemical industry* • *Research facilities* • *Water* • *Energy* • *Bless you* • *Information and communication technologies* • *Transport* • *Feeding* • *Financial and tax system*	**N.C.I.P.C** National Center for Infrastructure Protection and Cybersecurity	http://www.cnpic.es

United States of America	**16 Strategic Sectors** • *Chemical* • *Communications* • *Dams/hydroelectric plants* • *Emergency services* • *Financial service* • *Government facilities* • *Information technology* • *Transport system* • *Commercial facilities* • *Manufacturing* • *Defense industrial base* • *Energy* • *Agriculture and food* • *Health and public health* • *Nuclear reactors, radioactive materials and waste* • *Water and treatment plants*	**C.I.S.A.** Cybersecurity & Infrastructure Security Agency	https://www.cisa.gov/critical-infrastructure-sectors
United Kingdom	**9 Strategic Sectors** • *Communications* • *Emergency services* • *Energy* • *Financial services* • *Feeding* • *Government* • *Bless you* • *Transport* • *Water*	**C.P.N.I.** Centre for the protection of National Infrastructure	https://www.cpni.gov.uk/
French	**12 Strategic Sectors** • *Feeding* • *Water management* • *Energy* • *Finance* • *Transport* • *Electronic, audiovisual and information communications* • *Industry*	**G.S.D.N.S.** General Secretariat of Defence and National Security	http://www.sgdsn.gouv.fr/

	• *Health* • *Space and research* • *Civilian activities* • *Military activities* • *Legal activities*		

Table 27: Comparative table of the different classifications made by different countries for strategic sectors.

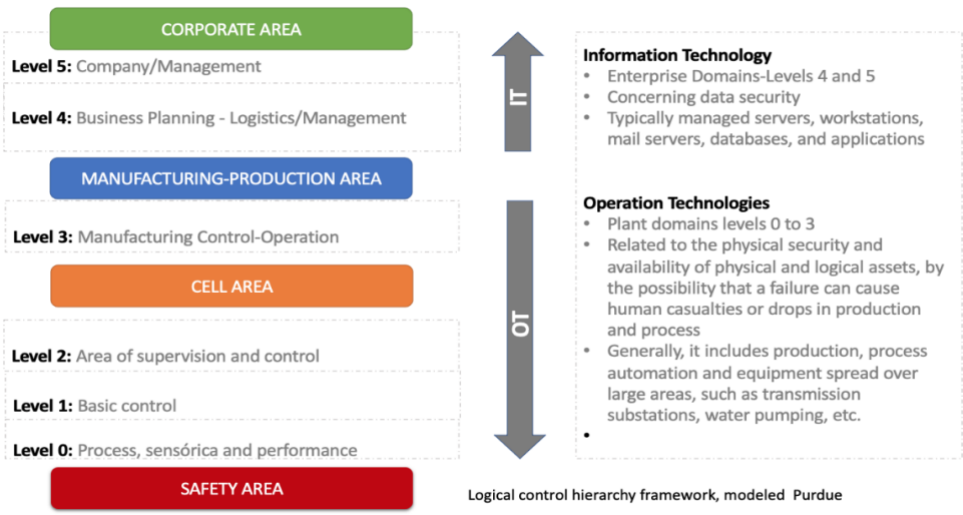


Figure 128: Logical framework of control hierarchy, according Purdue model.

The increase in communications due to the exponential increase in those of intelligent elements and the need to integrate process data into corporate systems and applications, have made IT appear and burst strongly into industrial environments. This aspect is clearly reflected in the Purdue model graphic below with a clear division of the logical framework of the control hierarchy (Figure 128).

Many companies have faced this dependency by creating their own support teams within business units, being different and separate from their own IT departments. From this action arises dualities between tasks and resources from personnel that can lead to problems resulting from the ignorance of functional disintegration and coordination and the lack of understanding among departments whose functions in origin become

similar. These differences and separations generate an increase in the risk of management and compliance actions, tasks that OT engineers are not too accustomed, and for which IT staff have wider experience. For these reasons, it is essential that both areas understand each other and collaborate together. It is clear that behind this defense of the integration between IT and OT, benefits are declared and their associated dangers are inherited.

As benefits we have:

- *A considerable improvement in automation and information reported by sensors.*
- *Increased control over distributed operations.*
- *More efficient systems in their response times and structure.*
- *An increase in efficiency and effectiveness due to better and more information.*
- *Improvement before decision-making based on more accurate information in a timely manner.*
- *An increase in customer satisfaction, as a result of proactive maintenance and reduced unavailability times.*
- *Advance of the satisfaction of the participants by having better flows of information.*
- *Clear and well-defined policy objectives.*

On the other hand, there are the dangers associated with IT that, therefore, are transferred to the area of operation by the convergence explained above. Advances in IT are providing industrial control systems with a great capacity for interconnection, adaptability and extension of production areas. However, the use of communication networks and this existing intercommunication makes industrial control systems highly vulnerable, considerably increasing their exposure area to possible

cyberattacks.[117] It is therefore essential to develop methodologies for identifying and tracking vulnerabilities, classifying prevailing systems and assets in critical infrastructures, regardless of their level of complexity, scalability and heterogeneity.

7.3. Concept of cybersecurity in industrial environments

As a consequence, and logical evolution of what was previously reported, approximately two decades ago, numerous organizations belonging to the commercial and industrial sectors began a digital evolution by interconnecting their IT with their OT.

Part of this interconnectivity was done using public communication networks, such as the Internet, for traditional IT systems. In the same way, OT systems were obtaining connection capacity from different devices outside the production process, according to their purest definition, which would give rise to the concept of IoT: sensors, endpoint-devices[118], human-machine interfaces Programmable Logic Controller, PLC[119] y Remote Terminal Unit, RTU[120].

In recent years there has been a proliferation of IoT devices and technologies, considerably increasing the number of elements and

[117] A cyberattack or computer attack, is any offensive maneuver of deliberate exploitation that aims to take control, destabilize or damage a computer system, which can be the attacker, an individual or organization.

[118] The *end-point,* also known as a terminal or endpoint, is any remote computing device that communicates with a network to which it is connected.

[119] A programmable logic controller *(PLC)* or programmable automaton is a computer used in automatic engineering or industrial automation, automate electromechanical, electropneumatic, electrohydraulic processes.

[120] A remote terminal unit (RTU) is a microprocessor-based device that allows process-independent signals to be obtained and information sent to a remote processing site.

functionalities. While this interconnectivity has helped improve collaboration, reliability, efficiency, availability, maintenance and productivity in their operating environments, cybersecurity has barely been taken into account. This lack of planning has resulted in an increased risk across the attack surface, offering more and better opportunities to attackers, malicious code creators and cybercriminal groups, which has been confirmed in view of the number of successful cyberattacks (Black-Energy, WannaCry y Petya, [URL- 07, 2018]) which have occurred in different industrial sectors (energy, transport, manufacturing, health, etc.) over the last few years.

Nowadays, it is common for cyberattacks to be carried out by multidisciplinary teams with knowledge of IT and the operation of the technological architecture of the industrial system under attack. In this way, not only would there be the ability to access the industrial control system, but also the most critical and sensitive parts of the industrial process would be identified, so that sabotaging it could cause serious damage that would affect the production of the industrial plant, the installation itself and even affect people's health.

There have already been cases (e.g., cyberattack in Ukraine 2015, [URL-08, 2015]) where industrial control systems were stopped and damaged due to attackers compromising the OT environment, accessing through IT infrastructures.

Consequently, and given the increase of cyberattacks suffered in organizations, cybersecurity has become an important issue in the agenda and priorities of board members, directly impacting on a significant increase in budgets dedicated to cybersecurity IT and OT. This marks a turning point in the concept of cybersecurity as a participatory process in each and every one of the stages and areas involved in any organization.

Thus, by way of summary and to complete the above, industrial cybersecurity encompasses several actions, addressing the prevention, monitoring and improvement of the resistance of industrial systems and their recovery from hostile or unforeseen actions, which may affect the proper functioning of industrial processes, being considered this industrial cybersecurity as a process that must be present in each and every one of the cycles involved in the industrial control systems.

7.4. Importance of cybersecurity in industrial environments

In this context and as a direct implication of the topic discussed in this Doctoral Thesis, another problem immersed in the area of industrial cybersecurity corresponds to the absence of specific standards and regulations for IoT technologies, which makes difficult their correct planning and execution. In addition, some cybersecurity models commonly used in the OT environment may not have been properly integrated into the lifecycle of IoT devices and platforms.

Repeatedly, the prevailing approach to cybersecurity in the OT environment is to implement solutions and technologies designed for IT. Unfortunately, this does not always work and has sometimes led to problems with equipment and devices in the operational plants. Both environments have heterogeneous views on cybersecurity and its applicability, as they have different business needs. As a result, common IT technologies, methodologies or procedures are misapplied in OT environments, which can lead to self-declarations of service and other complications caused by the organization itself.

As an example, the management and use of common IT resources and applications for intrusion testing, or network mapping tools can affect OT

systems, such as old PLCs or CPUs. Similarly, the traditional application of antivirus software, antimalware on field devices, HMI or traditional control systems, can affect its availability and performance. While it is true, as has been mentioned, that there has been a significant increase in the number of cyberattacks suffered in all sectors of the industry, very few of these incidents have been able to be related to cyberspace, which significantly demonstrates the limitations in computer forensic analysis capabilities in industrial control systems. This gap is expected to become even more complicated with the advent of IoT in general and IIoT in particular.

Network monitoring through end-OT-end security event correlation (from IT to OT) is an opportunity to implement an active defense and threat identification strategy for the entire organization. It is assumed that many industrial processes will need coexist with unsafe products (both devices and applications) for years. Therefore, one of the points with the highest priority address is the premature identification and correction of existing gaps in security requirements between both environments, to develop compensation and forecasting controls, as well as constitute a comprehensive cybersecurity plan for the entire organization.

Another aspect to improve is the empowerment, collaboration and creation of multidisciplinary teams that help advance in this lack of adequate and efficient contribution among the work teams of these environments. In addition, promoting awareness-raising and training sessions designed specifically for professionals working in the IT and OT convergence zone, multidisciplinary working groups need to be established, so that all aspects of a security problem in the industrial field are considered. In parallel, a common culture and language must be developed in an environment of cooperation and mutual understanding, since nothing separates people more than the language used. That is why the management of cultural

aspects is the essential preliminary step create a truly safe industrial environment.

Undoubtedly, decisive steps must be taken in the right direction to solve the cybersecurity aspects and concerns related to the adoption of new technologies and platforms offered by cloud computing and IIoT. The associated complexity lies, specifically, in the management of the cybersecurity of the data, communications, services, etc. provided by the large number of "smart" devices that will be implemented in industrial environments. The IIoT attack surface is expected to be expanded significantly[121].

Finally, being aware that there are not miraculous to solve the cybersecurity problems associated with the IT/OT convergence, at least an initial plan is suggested by applying the following set of measures:

- *Basic security controls must be implemented in all layers and environments in your organization.*
- *The cybersecurity of both environments (IT/OT) must be managed by a final manager and must be aligned with the guidelines set from the management.*
- *The technologies and threats in both environments must be clearly understood. IT technologies may not necessarily work in the OT environment. In addition, the threats may be different.*
- *Have a clear discovery and management plan. If you do not know what you have, you will not be able to know its weaknesses and therefore its defence capabilities.*

[121] Cloud computing , also known as cloud services or simply "the cloud", is a paradigm that allows you to offer computing services over a network, which is usually the Internet.

- *Periodic risk analysis should be performed in both environments to identify vulnerabilities and ensure that appropriate security controls are in place.*
- *Organizations should consider regulations from both environments such as NIST 800-53 for IT [URL- 09, 2017], NIST 800-82 [URL- 10, 2015], & ISA / IEC 62443-1-2 [URL- 11, 2017], for Industrial Control Systems (ICS) and OT.*
- *Develop SCI-specific policies and procedures that are consistent with IT cybersecurity, physical security, and business continuity.*

7.5. Cybersecurity and cyber-resilience

As a direct consequence of the evolution in the terminology that is breaking into the OT and its growing importance in roles assumed by its advancement, this section concisely analyzes the concept of a cyber-resilient industry, by functional necessity and operational security. This concept serves to qualify the one who has the ability to prevent, detect, contain and recover the affected system before an unwanted action, minimizing the exposure time and the impact or final damage.

This thinking is closely linked that of cyber-risk, cybersecurity and the operational continuity of the technologies resident in the management areas of industrial control systems. This means not only being prepared to react against adverse situations, but also having the ability to be preventive against possible disruptions, which are threats for these systems.

Thus, the study presented in this Thesis focuses on obtaining this capability, which gives a relevant importance to industrial environments because they need a high availability capacity, highlighting the ability to foresee future logical, operational and cyber security events.

7.6. Critical Infrastructure

As a concept that represents the importance of protecting all those systems, networks, production plants, etc., the critical infrastructure (CI) arises. The meaning of critical infrastructure gives a high rate of differentiation those designated in such a way, distinguishing them from those not catalogued in that way.

The designation of CI is used by the different States to detail, define and catalog facilities and systems that provide essential services and whose disruption does not allow alternative solutions. Their grouping is intrinsically carried out in strategic divisions. These groups, specifically in Spain and according to the PCI Law (Law on the Protection of Critical Infrastructures), issued on 8/2011, dated April 28th [URL- 12, 2011], the CIs are classified in 12 sectors, which are all those that obtain their role as essential for national security or for the whole of the country's economy (energy, information technologies, transport, water, health, food, finance, nuclear, chemical, research, space, and administration).

The approach to the protection of these infrastructures arises as a response by governments the need to protect the complex system of infrastructures that support and enable the normal functioning of the productive sectors, management and the daily life of society.

The events that have occurred during the last two decades, attacks of September 11th- 2001, the terrorist attacks in Madrid of March 11th- 2004, the recent acts of cyberespionage, carried out by States (Mandiant report) [URL- 13, 2013] or by corporative spies, passing through the threats of Anonymous, Wikileaks and the effects of malware such as Stuxnet, have led most governments to include in their agendas the development of national

cybersecurity strategies as well as the deployment of specific protection measures[122-123-124].

These incorporations in the government's strategic plans converge to guarantee the security and stability of their critical infrastructures, having a direct impact on the social and state stability of each of them.

With this objective set and as premises in the lines of action for obtaining an action plan for strategic and tactical protection, the different countries have addressed this problem under different perspectives, being able to group these into:

- *Development of a strict and clearly defined regulatory framework.*
- *Strengthening relations between public and private entities.*
- *Establishment of a basic regulatory framework accompanied by a series of measures to enhance public-private relations, as a complement to the previous points.*

In any case, the objective to be achieved for the protection of critical infrastructures corresponds to the development, implementation and improvement of the appropriate security measures, both in its physical and logical/cyber aspects, which must be undertaken by the operators who own or are responsible for their management, in order to guarantee an adequate level of protection.

[122] The Mandiant report offers an enormous amount of information that reveals a great deal of work (both technically and in terms of the number of resources allocated), and whose quality can be considered as solid at a technical level.

[123]Emerged from the imageboard 4chan and the Hackers forum ; at first as a fun movement. Since 2008 Anonymous has been demonstrating in protest actions in favor of freedom of expression, access to information, the independence of the Internet and against various organizations.

[124] It is an international non-profit media organization that publishes through its website anonymous reports and leaked documents with sensitive content in the public interest, preserving the anonymity of its sources.

The System and Infrastructure of Knowledge for Real Experimentation through of Cells of Industrial Automation (SIKRECIA), developed as the main element of this thesis, provides new contributions for the improvement of research, development, simulation and testing of the operation of these systems, as well as the ability to predict the behavior of a specific system in real industrial production, providing operational, tactical and strategic value for the defense of CIs.

The different scenarios recreated through SIKRECIA have the ability to anticipate the new threats that affect SCI of critical infrastructures. Being an open system, SIKRECIA can use components from different industrial manufacturers to cover existing architectures in the process industry.

The different scenarios recreated through SIKRECIA have the ability to anticipate the new threats that affect SCI of critical infrastructures. Being an open system, SIKRECIA can use components from different industrial manufacturers to cover existing architectures in the process industry.

7.7. Thesis structure

After a detailed introduction of the evolution of control systems, from their primitive appearance to the present day, in which certain shortcomings have been revealed as a consequence of the evolution itself, the lines of work carried out in the research presented here are described.

This section summarizes the contents of the chapters of this Thesis.

In Chapter 1, after a brief introduction into the evolution of industrial environments and the classification of these historical periods according to the industrial revolutions that have occurred, the concepts of Information Technologies (IT) and Operating Technologies (OT) have been defined, disserting for each of these areas the emerging problems as a result of their

convergence. Thus emerge the concepts of cybersecurity and cyber-resilience in the industrial field. The typification of industrial control and automation systems arises under the legal protection of their classification as Critical Infrastructures. There is a turning point for the cataloguing, staging and protection of these infrastructures and their respective control systems after the terrorist attacks of September 11th 2001[125].

Chapter 2 presents the objectives that serve as support for the research developed in this thesis. These objectives are broken down and classified into general and specific. As a result, the starting hypotheses are posed and detailed, providing the motivations for the realization of the research. The content of the rest of the chapter deals with the description of the relationships for an adequate adaptability and effectiveness of the infrastructure proposed for the improvement of cybersecurity in operational environments of industrial automation systems. It will be detailed in the final part of the chapter, the methodology developed for the research, which will be particularized in the content of chapters 4 and 5 as a result of the research carried out.

Chapter 3 comes to describe a deep and detailed state of the art concerning the bases that support the study carried out in this thesis and that have been described in the previous chapter. The study begins with the current state of maturity of the ICSA, describing the analysis carried out of the main international reference frameworks for the implementation and evaluation of the maturity of operational systems. NIST and C2M2 stand out

[125] The September 11th 2001 attacks, also known by the names "11S" and "11-S" (9/11" "11/9"), were a series of four suicide terrorist attacks committed on the morning of Tuesday, September 11, 2001, in the United States by the jihadist al-Qaeda network that, by hijacking commercial aircraft to be hit by various targets, killed 2,996 people.

and have been taken as basic examples and references considered for their deployment in SIKRECIA. A detailed study is then made of the scope and of the parties involved that come to limit the area of research that has been chosen. All those new exposures, vulnerabilities, threats and risks which the SCI are being forced are detailed, given their very high interoperability and interconnection. Finally, the rest of the chapter is dedicated to the exposition and analysis of different tools and techniques existing today, whose mission is to combat and prevent possible disruptions as a result of cyberattacks or deficient / erroneous configurations in the OT environment.

Chapter 4 describes analytically the first of the two investigations carried out and that corresponds to the case raised as the main research developed in this thesis. It begins by carrying out a descriptive analysis of each and every one of the sub-systems that make up SIKRECIA. The next level corresponds and mentions the methodology and materials implemented for its deployment, delving into the specific functionalities in an individualized way. After having erected a complete functional analysis, the specific programming executed through the engineering tool taken as a reference is detailed, which facilitates the creation and programming of the environments in IACS and is deployed and used in industrial contexts. To conclude the chapter, the results obtained through SIKRECIA and CVSS V 3.0 are presented and analyzed as tools for the improvement of cyber-resilience, detailing and exposing the conclusions reached.

Chapter 5 describes and studies several practical aspects obtained because of the research developed in the Center for Cyber-excellence of NATO, located in Tallinn (Estonia) and that corresponds to the second case of research executed and described in this thesis. This work has been developed within the search and study of vulnerabilities in electricity generation and distribution systems. A complete chapter has been dedicated

to the research detailed in this section, as a result of the high degree of particularity that the electricity sector has, specifically in the areas of generation and distribution. Due to its special nature, a specific execution environment is necessary in terms of the engineering elements and industrial programming software for its deployment and configuration. This reason directly influenced and was paramount in carrying out the choice of the existing laboratory at the NATO Cyber Defence Centre of Excellence (CCDCoE) for the research detailed in Chapter 5.

Chapter 6 collects a summary of the main conclusions and contributions of this thesis in the field of engineering and, specifically, in the area of cybersecurity of the ICSA in Critical Infrastructures, as well as the proposals of future lines of work on it.

This report ends with a complete bibliographic index, a compendium of appendices, lists of programming source codes, references to URLs of documentary repositories, and a list of symposia in which we have participated as a result of the research developed.

Chapter 7 corresponds to a global summary of the work carried out throughout the research presented in this Doctoral Thesis including the compendium and analysis of the conclusions obtained from the research developed.

7.8. Synopsis

The advances in Information Technologies (IT) are providing Industrial Control Systems (ICS) with a great capacity for interconnection and adaptability. However, the use of communication networks makes ICS highly vulnerable. Consequently, it is essential to develop methodologies for the identification and subsequent classification of the ICS that intervene in

critical infrastructure assets with any level of complexity, scalability and heterogeneity. The System and Infrastructure of Knowledge for Real Experimentation by means of Cells of Industrial Automation (SIKRECIA), described in this work, provides new capabilities for research, development, simulation and testing of the functioning of these systems, and the ability to fore-see the behavior of a specific system in industrial production. The scenarios recreated through SIKRECIA have the ability to anticipate new threats that affect the ICS of critical infrastructures. Using SIKRECIA, a specific vulnerability of a programing logic controller, (PLC) has been verified through the engineering programmed for the management of a traffic light control system. The results obtained demonstrate the high dependence between IT and OT systems and therefore the importance of being able to recreate those environments before entering into operation.

As SIKRECIA is an open system, it can use components from different industrial manufacturers to cover the existing architectures in the process industry.

7.9. Chapter 1, summary

To carry out a correct recapitulation of what was reported in this research and fruit of the investigations that in the corresponding sections have been formally detailed, it is necessary to introduce historically the evolution that occurred in the SCI as described in previous sections. Since the beginning of time, the human being has been looking for methodologies supported by the creation of tools and machinery that would facilitate and make his life more comfortable and bearable. This has led us to be able to adapt our evolution as a species to this day.

Because of this, the introduction of the first section has been initiated by granting a timeline affiliated to the main relevant facts associated with what we know today within the definition of "industry". These milestones have given rise to the so-called industrial revolutions, which mark a before and after the adaptation of the human being to his way of materializing his work, in a safer and more efficient way.

As a result of these industrial revolutions, a new concept emerges, which is that of the technologies of the operation (OT). it will come to be defined as the application of engineering to obtain a faster, simpler, more efficient, and safer production.[126]

It has been described the influence that is exerting the interaction of information technologies (IT) with those of the operation, of themselves separately, as well as the problem that, from the point of view of cybersecurity, is emerging today and in full expansion of the 4th Industrial Revolution by its convergence and high connectivity to the outside world. As a result of this interconnection, new exposures to the outside world emerge and therefore the needs of protection against these new risks appear. As consequence of it arises the need to enhance the cybersecurity and cyber-resilience of CIs.

Finally, as an advance of the importance of these systems, the concept of critical infrastructures has been described as well as its scope of applicability, giving as an example the classification that has been chosen and that have been developed in different countries, thus giving a different point

[126] Engineering is the discipline and profession that applies technical and scientific knowledge and uses natural laws and physical resources, to design and implement materials, structures, machines, devices, systems and processes to achieve a desired goal, but that meets the specified criteria.

of view depending on the classification, but converging at the same time in the identification as CI.

For the end of the introduction, and with the aim of giving fluidity to the understanding of the coming sections, we proceed to detail chapter by chapter its structure and content.

7.10. Chapter 2, summary

In this chapter we have described the works contributed by the research developed in the thesis. It has begun by introducing the concepts of OT and IT throughout the history of automation, describing the relevance of these separately, as well as the problem that, from the point of view of cybersecurity, is emerging today and in full expansion for its convergence and high connectivity to the outside world.

It has gone a step further, clarifying the relevance that these OT have within the national critical infrastructures, making them worthy of an in-depth study on their capabilities of prevention and anticipation against a cyberattack, holding an important role within the certification systems proposed by the European Union.

As a result of the reflections raised from this new problem, the hypotheses that motivated the research presented and that gave rise to the general and specific objectives that were the origin of the structure followed in this research work have been detailed.

Mention has been made to the investigations carried out and that have led to the search for vulnerabilities in industrial control platforms and devices of the main worldwide manufacturers and that are, in turn, deployed in strategic/critical infrastructures of electricity distribution. This sector, the electrical sector is extremely important for the rest of national and

international strategic sectors for its critical contribution to the operation of the rest of the components and ICSA.

Similarly, we have analyzed the direct involvement between conservative cybersecurity thinking (through its applicability in IT environments) and the one corresponding to the holistic analysis of the definition and applicability of cybersecurity in the field of TO [Tripathi S., 2021].

Below, we have described the two studies carried out with the methodology developed and that constitute the core of this thesis. The first analyzes the field of industrial process cybersecurity through the analysis of the possibilities, interconnection capabilities, adaptability and dependencies created by IT towards OT [González S., 2020]. The second study provides the data obtained after the performance of pentesting tests and the search for vulnerabilities in industrial control elements of the area of electricity generation and distribution, from different manufacturers and deployed in the distribution part of the energy sector of European critical infrastructures.

Throughout this chapter we have analyzed the situation and the state of maturity of cybersecurity in SCI, performing an in-depth analysis of the state of the art. For this reason and given the speed that industrial control systems are being influenced by everything related to IT and by their complexity and diversity between IT and OT, the content of this chapter has increased considerably.

As a result of the digital and interconnection evolution to which the industry is being called upon, new scenarios arise that entail certain threats and, consequently, involve certain risks. Knowing these risks, as well as assessing the level of tolerance within each organization, is not an easy task, especially given the involvement that SCI have in critical infrastructures. That

is why regulations and standards arise to support and legislate these new paradigms.

As reflected in this chapter, numerous entities, organizations, and regulatory bodies that are working in their respective fields coexist to generate procedures to improve the cybersecurity of these environments. These initiatives, already in possession of a wide spectrum of possibilities, are focused on obtaining operational information of the latest techniques used by the attacking agents. One of the best ways to protect industrial systems is to know their own weaknesses and, in turn, to learn about the techniques of attacks intervened and of which they have been targeted.

For this reason, the last section of this chapter has been dedicated to honeypots, since combined with the testing laboratories explained in previous sections, they form a perfect symbiosis to the improvement of detection and resilience capabilities.

SIKRECIA comes to collaborate directly in this area since it meets qualities such as the capacity for prior analysis of infrastructures and the enhancement of their cyber-resilience capacity.

For this same reason, Chapter IV is focused on the development of a multipurpose industrial automation cell deployed within an IT system for obtaining anticipatory and resilience capabilities and for the improvement of cybersecurity in the area of automation in operational environments. In turn, Chapter V will show a concrete and exhaustive research carried out in smart and new generation electricity grids (Smart Grids), where searches were made for vulnerabilities of "0 day" in platforms and devices of the main manufacturers of industrial control systems worldwide and that are, in turn, deployed in strategic/critical infrastructures.

7.11. Chapter 3, summary

Throughout this chapter we have analyzed the situation and the state of maturity of cybersecurity in ICS, performing an in-depth analysis of the state of the art. For this reason and given the speed with which industrial control systems are being influenced by everything related to IT and by their complexity and diversity between IT and OT, the content of this chapter has increased considerably.

As a result of the digital and interconnection evolution to which the industry is being called upon, new scenarios arise that entail certain threats and, consequently, involve certain risks. Knowing these risks, as well as assessing the level of tolerance within each organization, is not an easy task, especially given the involvement that ICS have in critical infrastructures. That is why regulations and standards arise that come to support and legislate these new paradigms.

As reflected in the chapter, numerous entities, organizations and regulatory bodies that are working in their respective fields coexist to generate procedures that improve the cybersecurity of these environments. These initiatives, already in possession of a wide spectrum of possibilities, are focused on obtaining operational information of the latest techniques used by the attacking agents. One of the best ways to protect industrial systems is, first of all, to know their own weaknesses and, in turn, to learn about the techniques of attacks intervened and of which they have been targeted.

Because of this, the last section of Chapter 3 has been dedicated to honeypots, since combined with the testing laboratories explained in previous sections they form a perfect symbiosis to position themselves in the improvement of detection and resilience capabilities.

SIKRECIA comes to collaborate directly in this area since it meets main qualities such as the capacity for prior analysis of infrastructures and the enhancement of their cyber-resilience capacity.

Consequently, the next chapter (4th) is focused on the development of a multipurpose industrial automation cell deployed within an IT system to obtain anticipatory and resilience capabilities and to improve cybersecurity in the area of automation in operational environments. In turn, Chapter V shows a concrete and exhaustive research carried out in smart and new generation electricity networks, where searches were made for vulnerabilities of "0 day" in platforms and devices of the main manufacturers of industrial control systems worldwide and that are, in turn, deployed in strategic / critical infrastructures.

7.12. Chapter 4, summary

The contributions of SIKRECIA for the improvement of cybersecurity and cyber-resilience of the ICSA have been developed and shown in this chapter. In the first place, the premises that justify why the cyber protection of industrial systems and automatisms and, consequently, their cyber-resilience should play a key role, resulting in the motivation for the creation and implementation of SIKRECIA.

Next, and to obtain the starting point of the tests to which the environments deployed for evaluation were subjected, each and every one of the components that make up SIKRECIA have been exhaustively detailed.

This dissociation of components comes to contribute and facilitate the understanding of the individual technical details and their contribution to the globality of the system, particularizing each of the roles assumed by

each component subsystem, defining in parallel their contributions to the confluence of IT and OT.

Then, and starting from the globality of the proposed architecture, certain parameters were specified, and several examples were executed, which were created through engineering software for the OT, in order to recreate a real system: a road and pedestrian traffic light management system. After obtaining the technical characteristics and its operational requirements, the system to be evaluated, and having carried out a previous approach to the potential problems associated with a specific environment, efforts were focused on the evaluation of the potential impact of a latent risk, opting for the use of the CVSS as system to provide a score according to the impact that a specific vulnerability could have.

For this purpose, a specific vulnerability of a Siemens SIMATIC S7 1200 PLC is taken as a reference and base element. This vulnerability highlights the capabilities of performing a previous study to obtain the severity of the impact of this vulnerability after applying SIKRECIA, clearly conferring improvements in cybersecurity and cyber resilience of the systems.

Finally, the factors that influence the variability of the environments are studied, characterizing it for the specific example chosen for this purpose.

7.13. Chapter 5, summary

The content of this chapter refers to the research actions carried out in a specific area, such as the transport and consumption of electrical energy. This sector has many connotations that give it a very special nature. Electrical energy is the fundamental pillar from which civilization and the development

of the human being as we conceive it today is sustained. For this reason, an entire chapter has been devoted to it.

Firstly, and having introduced the importance of the facts presented here, a new concept has emerged which has not been seen so far, but which will carry the weight and justification of the analyses carried out. This is the concept of smart grids.

Next, the premises that justify why the cyber protection of the systems and automatisms involved within the smart grids, and of the systems that control, manage, and transport the electrical energy to its point of consumption, should play a key role. This section comes to be reinforced through a detailed procedure, where all the intervening elements are reflected, as well as the architecture deployed for this purpose.

Consecutively, and to obtain the starting point of the tests to which the environments deployed for evaluation were subjected, the communication protocols involved in these scenarios have been detailed, exhaustively. At the same time, special mention should be made to the fact that new risks and threats have appeared because of the paradigm shift experienced, a consequence of the transition between a purely "electric" approach to an "electrical + data management and control" approach in the area of energy generation and transport. After obtaining the technical characteristics and operational requirements of the system to be evaluated as a whole and, in particular, the communication protocols to be used, and having carried out a previous approach to the potential problems associated with the specific environment, efforts were focused on the search of vulnerabilities in the communications between devices within the framework of the architectures and standards deployed in the smart grids.

To conclude, all those parameters and weaknesses that have been highlighted within this research have been shown, focusing mainly on those

that, intentionally or unintentionally, would result in highly dangerous consequences for the environment, systems and even human lives.

To obtain the data presented here, real elements of electrical infrastructures have been necessary, as well as highly specialized software in the sector. All these elements are owned by the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia (CCDCoE).

7.14. Chapter 6, summary

In this research, the starting point was fixed in the conceptual definition of the models of industrial control systems and their original situation completely isolated from any collaborative environment. These environments were designed for incorruptible availability but without considering the concepts of integrity and confidentiality in the data required or provided, as a consequence and necessity of its operation.

Progressively, and because of the emergence of new and diverse energy elements for use in automation, as well as new ways of carrying out processes in industry, there have been significant changes in these systems that have given rise to industrial revolutions.

Already in the current era and because of the technological contribution of IT to the operation of OT, a new paradigm is defined directly related to the era of interconnection in which we are currently involved. Given this dizzying adaptability and affinity, new threats emerge to which ACSI and, therefore, critical infrastructures are exposed. It is for these reasons that the preventive capacities of these environments must be enhanced to avoid disruptions, intentional or not, of these CI, since

otherwise, a serious risk is assumed in all those parameters involved as horizontal criteria of criticality defined in Law 8/2011 of PCI[127].

The real versatility of the system is given by the high adaptability for the incorporation of as many IAC as manufacturers of industrial control systems and automatisms exist. In turn, providing all the software involved in these networks allows to increase the quality of vulnerability analysis. Consequently, the main contribution of this research, materialized through SIKRECIA, is the provision of a secure framework that will help to obtain an analysis that demonstrate the true state of maturity of an industrial architecture that users will deploy according to their research needs.

7.15. Chapter 7, summary

The content of this chapter corresponds to a complete recapitulation of all the study carried out in the Doctoral Thesis developed. It includes a section by chapter of the evolution of industrial systems and automatisms developed by humans. It begins with a historical introduction of its evolution, going through the needs that emerge given the dependence between IT and OT.

It concludes with the concrete research developed and that provide, after the evaluation of the objectives raised and achieved as a result of the initial hypothesis, the conclusions and future lines of research proposed.

[127] It should be understood that the horizontal criteria of criticality correspond to those identified by the PIC Law that intervenes in the cataloguing of the severity and consequences of the disturbance in the CI: number of people affected, economic impact, environmental impact and public and social impact.

7.16. Final conclusions

Once the results obtained have been examined and evaluated, the main conclusions of the research work carried out have been:

1) This paper has presented the development of a new concept of process simulation in industrial environments through learning by real experimentation, taking advantage of advances in the world of IT. Currently, with the increase in the presence of IT in the field of control and automation, industrial systems are exposed to a large number of new cyber-threats. Taking into account the important role played by infrastructures and services essential for the normal development and coexistence of society, it should be considered that the current and future lines of cyberattacks will derive from attempts to breach these facilities [Genge B., 2015].
2) It has been shown that it takes on a transcendental value to discard the idea that "security due to ignorance" corresponds to a valid method of protection against this type of attack. Therefore, it is very important to be prepared for possible eventualities through "practices and tests" [Stergiopoulss G., 2015], thus obtaining a high degree of resilience [Roldán G., 2017], [Chaves A., 2017]. At the same time, the importance of being able to obtain a high level of maturity and anticipation of the new vectors that will give access to cyberattacks in industrial control systems is highlighted, being the best defense against these new challenges training and previous experimentation in controlled environments.
3) At the same time, the application of theoretical knowledge without assuming the risk of implementing these analyses in production plants is remarkable, encouraging these environments

experimentation and analysis prior to implementations. All these practical capabilities have been shown in this Thesis using SIKRECIA through the use and evaluation of a vulnerable environment, finding this weakness duly documented and whose impact was relevant from the point of view of cybersecurity.

4) Through the applicability of SIKRECIA in the laboratory, the effectiveness of the preventive and reactive capacities has been verified, being completely neutralized the dangerousness of the vulnerability chosen as a proof of concept for the present study.

Similarly, in the chapter corresponding to the search for vulnerabilities in certain components and in the standards involved in the stages of generation and transport of electrical energy, relevant facts have been provided for the investigation. This sector has many connotations that give it a very special nature since electrical energy is the essential pillar on which the ICSA involved in the CI Are based. The electricity sector in general, and smart grids in particular, come to justify the key role that cyber protection must play within the systems and automatisms involved in these infrastructures. The fact of the appearance of new risks and threats as a result of the paradigm shift experienced, a consequence of the transition between a purely "electric" approach aimed at an "electric + data management and control" approach, in the area of energy generation and transport, comes to evidence this type of evaluation. Through the use of a real environment created for this purpose, assessment and design tests were carried out with the corresponding cybersecurity evaluations. Efforts were focused on the search for vulnerabilities in communications between devices within the framework of the architectures and standards deployed in smart grids. As a result, the existence of different security breaches of a critical nature was corroborated, both in deployed hardware devices and in

communication standards and proprietary engineering and management software.

7.17. Future lines of research

This subsection establishes the starting point for those actions that have been identified as possible points of continuity of this research. These future lines have been framed within two areas: those associated with SIKRECIA and those related to its application in the electricity sector.

7.17.1 SIKRECIA

The future lines of research in the field of prevention and resilience in cybersecurity in environments and ICSA detailed in this thesis go through:

- The incorporation and creation of new IAC from different manufacturers. In this way a heterogeneity in components is achieved, which guarantee a real approximation to the architecture of the existing industry.
- Obtaining connections through more complex and hybrid organizations, such as the National Network of Industrial Laboratories (NNIL) [URL- 116, 2021], others existing in various universities and research centers[128].
- Incorporation of the taxonomy of cyberattacks (Cyber Attack Taxonomy, CAT), [Intelligence-Led, 2019], as a model of analysis and representation of cyberattacks to be recreated by SIKRECIA. CAT's strategic model will help simplify the understanding and design of cyberattacks, standardize the interpretation of how actors operate, allow for faithful reproduction of actions carried out by attackers, and rule out solutions such as countermeasures. Thus, the functionality established in CAT fits perfectly

[128] The National Network of Industrial Laboratories is a platform of industrial laboratories NNIL, with the capacity to experiment and research solutions that increase the safety levels of national industrial infrastructures.

with the fundamental basis of the creation of SIKRECIA, which is to recreate and verify the ICSA, duly capturing and documenting each and every one of the phases in the seven layers of the maturity level detection models [Mavroeidis V., 2017], and remaining fully aligned with the recommendations of the European Commission, fruit of the incipient concern to promote the creation of certifying entities in industrial cybersecurity, and by extension to the CIOT.

- Promote, through this type of architecture, the constitution of criteria for a standardization aimed at obtaining a certification framework for the components of the ICSA in the area of cybersecurity at European level, affecting by extension their critical infrastructures.
- Promoting research for the incorporation of Blockchain technologies to improve authentication, communication and availability issues in ICSA.

7.17.2 ACSI involved in electric generation and transport

In the same way, future lines of research in this area of research go through:

- Enhancement of the recreation of hybrid test laboratories (manufacturers, and RTU models) for a real-world approach deployed in smart grids.
- Accession and obtaining access capacities to the laboratories of the main manufacturers of the RTUs.
- Research on the enhancement of security measures in the protocols and standards involved in communications, focusing efforts on the part of non-interference between encryption systems in the channels and the low tolerance in latency times required by the infrastructures of the sector.

- In-depth work on measures and control over the possibilities of the CPUs of the RTU, in favor of the improvement and reduction of times before encryptions in communications.
- In-depth evaluation of GOOSE and MMS in their network structure for improvements in communications, all aimed at enhancing levels of trust in end-to-end encrypted communications.
- Apply the methodologies studied in this thesis for the applicability of analysis methods in different communication protocols valid for these technologies.
- Carry out a study that allows to establish an effective training methodology, with which the best samples can be chosen to form a solid starting point towards change and/or adaptability in a new and safer communication protocol than those analyzed in this thesis.

Bibliografía

[Acero G., 1994]	Acero, G. H. (1994). «*Convertidores electromecánicos de energía*». Marcombo.
[Adamas K., 2021]	Adams K. y Heidarzadeh M., «A multi-hazard risk model with cascading failure pathways for the Dawlish (UK) railway using historical and contemporary data», *International Journal of Disaster Risk Reduction*, vol. 56, p. 102082, 2021, doi: 10.1016/j.ijdrr.2021.102082
[Adamu A., 2020]	Adamu A., Aliyu M., Muktar Y., Yaú N., Department of Computer Science, Yobe State University Damaturu, «Cybersecurity capability maturity models review and application», International Journal of Engineering & Technology, 9 (3) 779-784, 2020.
[Alheib M., 2016]	Alheib M. et al., «Improved risk evaluation and implementation of resilience concepts to critical infrastructure», DiVA, id: diva2:1322602, p. 344, 2016, [https://www.diva-portal.org/smash/get/diva2:1322602/FULLTEXT01.pdf.
[Anna S., 2016]	Anna S., Secure Infrastructure & Services Unit, «ENISA (European Union Agency for Network and Information Security), Stocktaking, Analysis and Recommendations on the Protection of CIIs», 2016.
[Ani J., 2020]	Ani, J. M. Watson, Green B., Craggs B., y Nurse J. R. C., Design Considerations for Building Credible Security Testbeds: «Perspectives from Industrial Control System Use Cases», *Journal of Cyber Security Technology*, vol. 0, n.º 0, pp. 1-49, nov. 2020, doi: 10.1080/23742917.2020.1843822
[Arinze U., 2016]	Arinze, U. C., Eneh, A. H., & Longe, B. O. « Overview of Nuclear Cyber Security Requirements for Nuclear Power Plants» https://conferences.iaea.org/event/181/contributions/15920/attachments/8409/11124/Overview_of_Nuclear_Cyber_Security_Requirements_for_Nuclear_Power_Plants__NPPs_.pdf
[Asklou N., 2020]	Asklou N. y Noureddine R., «Effects of proof tests on the safety performance of safety-instrumented systems», *International Journal of Industrial and Systems*

	Engineering, vol. 34, n.º 3, Art. n.º 3, 2020, doi: 10.1504/IJISE.2020.105740
[Axel D., 1999]	Axel D., CERN, Geneva, Switzerland y W.Salter, CERN, Geneva, Switzerland, «What is SCADA?», I*nternational Conference on Accelerator and Large Experimental Physics Control Systems, Trieste, Italy*, 1999. https://cds.cern.ch/record/532624/files/mc1i01.pdf
[Azuero A., 2021]	Azuero Á. E. A., «Significatividad del marco metodológico en el desarrollo de proyectos de investigación», *Revista Arbitrada Interdisciplinaria Koinonía*, vol. 4, n.º 8 (Julio-Diciembre), pp. 110-127, 2019, https://dialnet.unirioja.es/servlet/articulo?codigo=7062667
[Bakare A. 2020]	Bakare A. A., «A Methodology for Cyberthreat ranking: Incorporating the NIST Cybersecurity Framework into FAIR Model», University of Cincinnati, 2020. https://etd.ohiolink.edu/apexprod/rws_olink/r/1501/10?clear=10&p10_accession_num=ucin1583247043269043
[Bello R., 2020]	Bello R., Andrés W., Becerra M., y Andrés F., «Metodologías de evaluación del riesgo en ciberseguridad aplicadas a sistemas SCADA para compañías eléctricas», p. 14.
[Bencomo S., 2004]	Bencomo, S. D., «Control learning: present and future», *Annual Reviews in Control*, vol. 28, n.º 1, pp. 115-136, 2004, doi: 10.1016/j.arcontrol.2003.12.002
[CCN-CERT, 2021]	CCN-Cert., Centro Criptológico Nacional, «Aumentan los ciberataques a las infraestructuras críticas», 2021. https://www.ccn-cert.cni.es/eu/gestion-de-incidentes/lucia/23-noticias/140-aumentan-los-ciberataques-a-las-infraestructuras-criticas.html
[Cendoya A., 2016]	Cendoya A, National Cyber Security Organization: spain, CCDCOE, NATO Cooperative Cyber Defence Centre of Excellence Tallinn (Estonia), 2016.
[Cerezo F., 2015]	Cerezo F. y Sastrón F. «Laboratorios Virtuales y Docencia de la Automática en la Formación Tecnológica de Base de Alumnos Preuniversitarios», *Revista Iberoamericana de Automática e Informática Industrial RIAI*, vol. 12, n.º 4, pp. 419-431, 2015, doi: 10.1016/j.riai.2015.04.005
[Chacón J., 2015]	Chacón J, Vargas H., Farias G., Sánchez J., y Dormido S., «EJS, JIL Server, and LabVIEW: An Architecture for Rapid Development of Remote Labs», *IEEE Transactions on*

	Learning Technologies, vol. 8, n.º 4, pp. 393-401, 2015, doi: 10.1109/TLT.2015.2389245
[Charles M., 2006]	Charles M. Davis, J, «SCADA cyber security testbed development, in: Power Symposium», 2006. NAPS 2006. 38th North American, 2006, pp. 483–488.
[Chaves A., 2017]	Chaves A., M. Rice, S. Dunlap, J. Pecarina, «Improving the cyber resilience of industrial control systems», International Journal of Critical Infrastructure Protection 17 (2017).
[Chekari T., 2021]	Chekari T. R. Mansouri, y M. Bettayeb, «Real-time application of IMC-PID-FO multi-loop controllers on the coupled tanks process», *Proceedings of the Institution of Mechanical Engineers, Part I: Journal of Systems and Control Engineering*, p. 0959651820983062, 21d. C. 2021, doi: 10.1177/0959651820983062
[Chen Z., 2020]	Chen Z., Han Q.-L., Yan Y., y ZWu.-G., «[UPDATE ICS]How often should one update control and estimation: review of networked triggering techniques», *Sci. China Inf. Sci.*, vol. 63, n.º 5, Art. n.º 5, 2020, doi: 10.1007/s11432-019-2637-9
[Cherdantseva Y., 2016]	Cherdantseva Y. *et al.*, «A review of cyber security risk assessment methods for SCADA systems», *Computers & Security*, vol. 56, pp. 1-27, feb. 2016, doi: 10.1016/j.cose.2015.09.009
[Chiza L., 2021]	Chiza L., Cepeda J., Riofrio J., Chamba S., y Pozo M., «Dynamic Modelling and Co-simulation Between MATLAB–Simulink and DIgSILENT PowerFactory of Electric Railway Traction Systems», en *Modelling and Simulation of Power Electronic Converter Dominated Power Systems in PowerFactory*, F. M. Gonzalez-Longatt y J. L. Rueda Torres, Eds. Cham: Springer International Publishing, 2021, pp. 95-129. doi: 10.1007/978-3-030-54124-8_4
[Christiansson H., 2008]	Christiansson H. y Luiijf E. «Creating a European SCADA Security Testbed», en *Critical Infrastructure Protection*, Boston, MA, 2008, pp. 237-247. doi: 10.1007/978-0-387-75462-8_17
[Ciberseguridad, 2020]	Ciberseguridad © 2020, «De la Ciberseguridad a la Ciberresiliencia», *Ciberseguridad*, 2020. https://ciberseguridad.com/guias/ciberresiliencia/

[Committee T., 2014]	Committee T. S. G. I. P.-S. G. C., «Guidelines for Smart Grid Cybersecurity», National Institute of Standards and Technology, NIST Internal or Interagency Report (NISTIR). 7628 Rev. 1, sep. 2014. doi: https://doi.org/10.6028/NIST.IR.7628r1
[Council Directive, 2008]	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», 2008.
[Critical Infraestructure, 2016]	Critical Infrastructures and assessment of the need to improve their protection, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM: Jl0013&from=EN, 2016.
[De la Torre. L., 2016]	De la Torre L., Sánchez J. P., y Dormido S., «What remote labs can do for you», *Physics Today*, vol. 69, n.º 4, pp. 48-53, 2016, doi: 10.1063/PT.3.3139
[Del Canto J., 2015]	Del Canto J, M.A. Prada, J.J. Fuertes, S. Alonso, M. Domínguez, «Remote Labo- ratory for Cybersecurity of Industrial Control System», IFAC PapersOnLine 48, 29 (2015) 013-018, 2015.
[DHS U., 2009]	DHS, U. (2009). «Catalog of Control Systems Security: Recommendations for Standards Developers», Department Homland Security EEUU, 2009.
[Directive, 2008]	Directive 2008/114/EC «Identification and Designation of European Critical Infrastructures and assessment of the need to improve their protection», 2008.
[Directive, 2016]	Directive (EU), 2016/1148 of The European Parliament and of the Council of 6 July 2016 «Concerning measures for a high common level of security of network and information systems across the Union», 2016.
[Dondossola G., 2009]	Dondossola G., Deconinck G., Garrone F., y Beitollahi H., «Testbeds for Assessing Critical Scenarios in Power Control Systems», en *Critical Information Infrastructure Security*, Berlin, Heidelberg, 2009, pp. 223-234.
[Dormido S., 2013]	Dormido S., Sánchez J., y Morilla F., «Laboratorios virtuales y remotos para la práctica a distancia de la automática», p. 14, 2013.
[Eeten M., 2011]	Eeten M. V., Nieuwenhuijs A., Luiijf E., Klaver M., y Cruz E., «The State and the Threat of Cascading Failure Across Critical Infrastructures: The Implications of Empirical

	Evidence from Media Incident Reports», *Public Administration*, vol. 89, n.º 2, pp. 381-400, 2011, doi: https://doi.org/10.1111/j.1467-9299.2011.01926.x
[Elhay M., 2019]	Elhady M. Abdelghafar, M. El-bakry Hazem, Abou Elfetouh Ahmed, «Comprehensive Risk Identification Model for SCADA HindawiSecurity and Communication Networks, Jesús Díaz-Verdejo (Ed.), Volume 2019, Comprehensive Risk Identification Model fo SCADA System», hindawi.com/journals/scn/2019/3914283, 2019 In press, doi:10.1155/2019/ 3914283.
[European Commision, 2005]	European Commission, Green Paper on a European Program for Critical Infrastructure Protection, com 0576 final, 2005.
[European Commision, 2016]	European Commission, Introduction to the European IACS Components Cybersecurity Certification Framework (ICCF), Feasibility study and initial recommendations for the European Commission and professional users, 2016 http: //publications.jrc.ec.europa.eu/repository/bitstream/JRC 102550/jrc102550.pdf.
[European Commision, 2019]	European Commission, «The IACS Cybersecurity Certification Framework (ICCF). Lessons from the 2017 study of the state of the art». *EU Science Hub - European Commission*, 2019. https://ec.europa.eu/jrc/en/publication/iacs-cybersecurity-certification-framework-iccf-lessons-2017-study-state-art
[Farooq S., 2019]	Farooq S., M. SHussain. M. S., y Ustun T. S., «S-GoSV: Framework for Generating Secure IEC 61850 GOOSE and Sample Value Messages», *Energies*, vol. 12, n.º 13, 2019, doi: 10.3390/en12132536
[Fernández R., 2020]	Fernández R., «El Internet de las cosas (IoT)», *Statista*, 2020. https://es.statista.com/temas/6976/el-internet-de-las-cosas-iot/
[FIRST, 2018]	FIRST Improving Security Together, Standard, «Common Vulnerability Scoring System (CVSS), v3.0 Specification Document» (v1.8), 2018.
[FIRST CVSS, 2020]	FIRST, CVSS v3 Equations, https://nvd.nist.gov/vuln-metrics/cvss/v3- calculator/ equations, 2020.
[Francis R., 2014]	Francis R. y Bekera B., «A metric and frameworks for resilience analysis of engineered and infrastructure

	systems», *Reliability Engineering & System Safety*, vol. 121, pp. 90-103, 2014, doi: 10.1016/j.ress.2013.07.004
[Gannin A., 2020]	Ganin A. A. *et al.*, «Multicriteria Decision Framework for Cybersecurity Risk Assessment and Management», *Risk Analysis*, vol. 40, n.º 1, Art. n.º 1, 2020, doi: https://doi.org/10.1111/risa.12891
[Genge B., 2015]	Genge B., I. Kiss, P. Haller. «A system dynamics approach for assessing the impact of cyber-attacks on critical infrastructures», International Journal of Critical Infrastructure Protection 10 (2015).
[Georgios T., 2020]	Georgios T. (European Comission), «Recommendations for the Implementation of the Industrial Automation & Control Systems Components Cybersecurity Certification Scheme (ICCS) | ERNCIP Project», 2020. https://erncip-project.jrc.ec.europa.eu/documents/recommendations-implementation-industrial-automation-control-systems-components
[Gómez L., 2018]	Gómez L. y Najani A., «Monitoreo de rendimiento para la seguridad de VPN a través de PfSense y OpenVPN», 2018. https://cdigital.uv.mx/
[González S., 2020]	González S. G., Dormido S Canto, y Sánchez Moreno J., «Obtaining high preventive and resilience capacities in critical infrastructure by industrial automation cells», *International Journal of Critical Infrastructure Protection*, vol. 29, p. 100355, jun. 2020, doi: 10.1016/j.ijcip.2020.100355
[Group I., 2019]	Group I. D. M., «El 65% de los entornos de fabricación funcionan con tecnología obsoleta | Endpoint», *IT Digital Security*,2019. https://www.itdigitalsecurity.es/endpoint/2019/04/el-65-de-los-entornos-de-fabricacion-funcionan-con-tecnologia-obsoleta
[Hadbah A.,2014]	Hadbah A., T. S. Ustun, y A. Kalam, «Using IEDScout software for managing multivendor IEC61850 IEDs in substation automation systems», en *2014 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, nov. 2014,pp. 7-72. doi: 10.1109/SmartGridComm.2014.7007624
[Herrero D., 2020]	Herrero D., Villareal, Arguedas, Matarrita C., y Gutiérrez-Soto E.,«*Remote laboratories: Educational resources for remote experimentation in times of pandemic from the*

	students' point of view», nov. 2020, Accedido: feb. 17, 2021. https://rdu.unc.edu.ar/handle/11086/17090
[Hutchins E., 2011]	Hutchins E. M., Cloppert M. J., y Amin R. M., «Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains», p. 14, 2011.
[INCIBE-CERT (a), 2015]	INCIBE-CERT, « Amenazas en los Sistemas de Control Industrial.»,2015. https://www.incibe-cert.es/blog/amenazas-sci
[INCIBE-CERT (b), 2015	INCIBE-CERT, «Evolucionando la comunicación en la industria, protocolos de comunicación.», *INCIBE-CERT*, 2015. https://www.incibe-cert.es/blog/evolucionando-comunicacion-industria
[INCIBE-CERT (c), 2015	INCIBE-CERT, «La Ciberseguridad en la Industria 4.0 2015. https://www.incibe-cert.es/blog/ciberseguridad-industria-4-0
[INCIBE-CERT, 2019]	INCIBE-CERT, «Seguridad industrial 2019 en cifras, 2020. https://www.incibe-cert.es/blog/seguridad-industrial-2019-cifras
[Initiative J., 2015]	Initiative J. T. F. T., «Security and Privacy Controls for Federal Information Systems and Organizations», National Institute of Standards and Technology, NIST Special Publication (SP) 800-53 Rev. 4, ene. 2015. doi: https://doi.org/10.6028/NIST.SP.800-53r4
[Intelligence-Led, 2019]	Intelligence-Led «Cyber Attack Taxonomy (C@T)», posted in https://github.com/ fdeandres/CAT, 2019.
[James R., 2019]	James R., Damon Frezza, Burhan Necioglu, L. Michael Cohen, Kebbeth Hoffman, Kristine Rosfjord, «Interdependent Critical Infrastructure Model (ICIM): an agent-based model of power and water infrastructure», 2019.
[Jim M., 2010]	Jim M., «Simulation breaks out, in: Control Global», Sep-2010, pp. 52–61
[Kamran M., 2020]	Kamran M., «Role of cultural heritage in promoting the resilience of linear/critical infrastructure system with the enhancement of economic dimension of resilience: a critical review» *International Journal of Construction Management*, vol. 0, n.º 0, pp. 1-10, 2020, doi: 10.1080/15623599.2020.1711493

[Kaplan A., 2000]	Kaplan A., «Capacity building: Shifting the paradigms of practice madurity level», *Development in Practice*, vol. 10, n.º 3-4, Art. n.º 3-4, 2000, doi: 10.1080/09614520050116677
[Karnouskos S., 2011]	Karnouskos S. y Colombo A. W., «Architecting the next generation of service-based SCADA/DCS system of systems», en *IECON 2011 - 37th Annual Conference of the IEEE Industrial Electronics Society*, 2011, pp. 359-364. doi: 10.1109/IECON.2011.6119279
[Knapp E., 2015]	Knapp E. D. y Langill, Joel Thomas, «Industrial Protocol - ScienceDirect»2015. https://www.sciencedirect.com/topics/computer-science/industrial-protocol
[Knapp E. (a), 2015]	Knapp E.D. y Langill, Joel Thomas, «*Industrial Network Security- Securing Critical Infrastructure Networks for Smart Grid, SCADA, and other Industrial Control System*»*Second Edition*. SYNGRESS-ELSEVIER INC., 2015.
[Kochkin D., 2020]	Kochkin D., Sukonschicov A., y Akhmetov T. R., «Methodology of models based on modified Petri nets», en *Proceedings of the III International Scientific and Practical Conference*, New York, NY, USA, mar. 2020, pp. 1-4. doi: 10.1145/3388984.3390882
[Kornecki A., 2010]	Kornecki A. J. y Zalewski J., Safety and security in industrial control», en *Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research*, New York, NY, USA: Association for Computing Machinery, 2010, pp.1-4.: https://doi.org/10.1145/1852666.1852754
[Kriger C., 2013]	Kriger C., S. Behardien, y Retonda-Modiya J.-C., «A Detailed Analysis of the GOOSE Message Structure in an IEC 61850 Standard-Based Substation Automation System», *International Journal of Computers Communications & Control*, vol. 8, n.º 5, Art. n.º 5, ago. 2013, doi: 10.15837/ijccc.2013.5.329
[Kumar V., 2021]	Kumar V., Kumar, R. y Pandey S. K., «LKM-AMI: A Lightweight Key Management Scheme for Secure two Way Communications between Smart Meters and HAN Devices of AMI System in Smart Grid», *Peer-to-Peer Networking and Applications*, vol. 14, n.º 1, pp. 82-100, ene. 2021, doi: 10.1007/s12083-020-00921-6

[Lahza H., 2018]	Lahza H., Radke K., y Foo E., «Applying domain-specific knowledge to construct features for detecting distributed denial-of-service attacks on the GOOSE and MMS protocols», *International Journal of Critical Infrastructure Protection*, vol. 20, pp. 48-67, mar. 2018, doi: 10.1016/j.ijcip.2017.12.002
[Lee S., 2021]	Lee S., Abdullah A., Jhanjhi N. Z., y Kok S. H., «Honeypot Coupled Machine Learning Model for Botnet Detection and Classification in IoT Smart Factory – An Investigation», *MATEC Web Conf.*, vol. 335, p. 04003, 2021, doi: 10.1051/matecconf/202133504003
[Ley PIC, 2011]	Ley PIC, Gobierno de España, «Ley 8/2011, de 28 de abril, por la que se establecen medidas para la Protección de las Infraestructuras Críticas», BOE, núm. 102, 2011.
[Lezzi M., 2018]	Lezzi M., Lazoi M., y Corallo A., «Cybersecurity for Industry 4.0 in the current literature: A reference framework», *Computers in Industry*, vol. 103, pp. 97-110, 2018, doi: 10.1016/j.compind.2018.09.004
[Lu K., 2021]	Lu K.-D., Zeng G.-Q., Luo X., Weng J., Luo W., y Wu Y., «Evolutionary Deep Belief Network for Cyber-Attack Detection in Industrial Automation and Control System», *IEEE Transactions on Industrial Informatics*, pp. 1-1, 2021, doi: 10.1109/TII.2021.3053304
[Luiifj H., 2010]	Luiijf H., Nieuwenhuijs A. H., Klaver M. H. A., Van Eeten M. J. G., y Edite Cruz, «Empirical findings on European critical infrastructure dependencies», *International Journal of System of Systems Engineering*, vol. 2, n.º 1, pp. 3-18, 2010, doi: 10.1504/IJSSE.2010.035378
[Mackiewicz R., 2006]	Mackiewicz R., & Heights, S. (2006, October). Technical overview and benefits of the IEC 61850 standard for substation automation. In *Proceedings of the 2006 Power Systems Conference and Exposition* (pp. 623-630).
[Mantha B., 2020]	Mantha B. R. K. y García de Soto B., «Assessment of the cybersecurity vulnerability of construction networks», *Engineering, Construction and Architectural Management*, vol. ahead-of-print, Art. Nº ahead-of-print, 2020, doi: 10.1108/ECAM-06-2020-0400
[Marcos M., 2004]	Marcos M., U. Gangoiti, D. Orive, E. Estévez, S. Calvo, J. Barandiarán,«Design and Validation of Industrial Distributed Control System, 43rd IEEE Conference on Decision and Control», decembre 14-17, 2004.

[Martínez L., 2009]	Martínez L., «Seguridad por oscuridad ¿verdadera seguridad?»2009. http://www.securitybydefault.com/2009/11/seguridad-por-oscuridad-verdadera.html
[Mashima D., 2021]	Mashima D., «16 - Securing smart-grid infrastructure against emerging threats», en *Solving Urban Infrastructure Problems Using Smart City Technologies*, J. R. Vacca, Ed. Elsevier, 2021, pp. 359-382. doi: 10.1016/B978-0-12-816816-5.00016-4
[Math W., 2020]	MathWorks, Simulation and model based design, (https://es.mathworks.com products/simulink.html), 2020.
[Mavroeidis V., 2017]	Mavroeidis V., S. Bromander, Cyber Threat Intelligence Model, An Evaluation of Taxonomies, Sharing Standards, and Ontologies within Cyber Threat Intelligence, European Intelligence and Security Informatics Conference (EISIC) (2017).
[Miranda J., 2014]	Miranda J. C., Chemin Netto U., DCoury. V., y Oleskovicz M., «Behaviour Evaluation of GOOSE Message Traffic between Power Substations: A POTT Scheme Case Study», *Journal of Control, Automation and Electrical Systems*, vol. 25, n.º 2, pp. 262-271, abr. 2014, doi: 10.1007/s40313-013-0087-1
[Morante N., 2019]	Morante N. y Rogger N., «Modelo de un sistema de gestión de seguridad de información SGSI, para fortalecer la confidencialidad, integridad, disponibilidad y monitorear los activos de información para el Instituto Nacional de Estadística e Informática INEI filial Lambayeque», *Universidad Nacional Pedro Ruiz Gallo*, nov. 2019. http://repositorio.unprg.edu.pe/handle/UNPRG/5935
[Mylrea M., 2017]	Mylrea M, S. N. G. Gourisetti and A. Nicholls, «An introduction to buildings cybersecurity framework, » 2017 IEEE Symposium Series on Computational Intelligence (SSCI), 2017, pp. 1-7, doi: 10.1109/SSCI.2017.8285228
[Nexon-Automation, 2019]	Nexon-Automation, «Maquinaria industrial: Estimación de su vida útil» *Nexon Automation*, 2019. https://www.nexonautomation.com/es/estimacion-de-la-vida-util-de-la-maquinaria-industrial/

[Noorizadeh M., 2021]	Noorizadeh M., Shakerpour M., Meskin N., Unal D., y Khorasani K., «A Cyber-Security Methodology for a Cyber-Physical Industrial Control System Testbed», *IEEE Access*, vol. 9,pp. 16239-16253, 2021, doi:10.1109/ACCESS.2021.3053135
[Office U.S.G.A., 2012]	Office U. S. G. A., «IT Supply Chain: National Security-Related Agencies Need to Better Address Risks», nº GAO-12-361, Art. nº GAO-12-361, 2012.
[Pérez E., 2009]	Pérez E. M., Acevedo J. M., y Silva C. F. «*Autómatas programables y sistemas de automatización / PLC and Automation Systems*». Marcombo, 2009.
[Peter M., 2007]	Peter M., S. Karen, R. Sasha, The Common Vulnerability Scoring System (CVSS) and Its Applicability to Federal Agency Systems, NIST Interagency Report 7435, Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899 8930, 2007.
[Quiang F., 2020]	Quiang F., Yao Y., Sheng C., y Yang W., «Interplay Between Malware Epidemics and Honeynet Potency in Industrial Control System Network», *IEEE Access*, vol. 8, pp. 81582-81593, 2020, doi: 10.1109/ACCESS.2020.2989612
[Real Decreto, 2010]	Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, BOE, núm. 25, 2010.
[Real Decreto, 2011]	Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de Protección de las Infraestructuras Críticas, BOE, núm. 120, 2011.
[Real Decreto, 2013]	Real Decreto 385/2013, de 31 de mayo, de modificación del Real Decreto 1886/2011, de 30 de diciembre, por el que se establecen las Comisiones Delegadas del Gobierno, BOE, núm. 131, 2013.
[Reda H., 2021]	Reda H. T. *et al.*, «Vulnerability and Impact Analysis of the IEC 61850 GOOSE Protocol in the Smart Grid», *Sensors*, vol. 21, nº 4, 2021, doi: 10.3390/s21041554
[Resilience Team ENISA, 2016]	Resilience team, ENISA (European Union Agency for Network and Information Security), Communication network dependencies for ICSS/SCADA Systems, 2016.
[Resilience Team ENISA (a), 2016]	Resilience T, ENISA (European Union Agency for Network and Information Security), Cyber Insurance: recent Advances, Good Practices and Challenges, 2016.

[Riccardo P., 2021]	Riccardo P., Alessandro De P., Francesco C., y Giulio G., «Simulation model for simple yet robust resilience assessment metrics for engineered systems | Elsevier Enhanced Reader», *ELSVIER*, vol. 209, 2021, doi: https://doi.org/10.1016/j.ress.2021.107467
[Rioshar Y., 2021]	Rioshar Y., Chuan G., y Faisal K., «A simple yet robust resilience assessment metrics, Elsevier Enhanced Reader», 2021. https://reader.elsevier.com/reader/sd/pii/S0951832019300687?token=DAEEB3B431084868F34DF4C07FB6B82C6F11B363A0C75463A4823FD94BF6B1EF6175CA9D58B66203C5136D193E98CF66
[Rodolfile N., 2019]	Rodofile N. R., K. Radke, y Foo E., «Extending the cyber-attack landscape for SCADA-based critical infrastructure», *International Journal of Critical Infrastructure Protection*, vol. 25, pp. 14-35, jun. 2019, doi: 10.1016/j.ijcip.2019.01.002
[Roldán G., 2017]	Roldán M., Almache-Cueva, Silva-Rabadão C., I. Yevseyeva, y V. Basto-Fernandes G., «A Comparison of Cybersecurity Risk Analysis Tools», *Procedia Computer Science*, vol. 121, pp. 568-575, 2017, doi: 10.1016/j.procs.2017.11.075
[Rosas W., 2020]	Rosas W. A., Medina F. A., y Mesa J. A., «Metodologías de evaluación del riesgo en ciberseguridad aplicadas a sistemas SCADA para compañías eléctricas», *Revista ESPACIOS*, vol. 41, nº 07, mar. 2020, Accedido: feb. 16, 2021. http://www.revistaespacios.com/a20v41n07/20410727.html
[Ross R., 2016]	Ross R., M. McEvilley, J. Carrier Oren, «Systems Security Engineering Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems», NIST (National Institute of Standards Technology) Special Publication 800 160, 2016.
[Sarry A., 2016]	Sarry A., Secure Infrastructure & Services Unit, ENISA (European Union Agency for Network and Information Security), Stocktaking. In *Analysis and Recommendations on the Protection of CIIs*». (2016).
[Saénz J., 2019]	Sáenz J., De la Torre L., Chacón J., y Dormido S., «A new architecture for the design of virtual/remote labs: The coupled drives system as a case of study», en *2019 24th*

	IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), 2019, pp. 769-775. doi: 10.1109/ETFA.2019.8869192
Sánchez J., 2002	Sánchez J., Morilla F., Dormido S., Aranda J., y Ruiperez P., «Virtual and remote control labs using Java: a qualitative approach», *IEEE Control Systems Magazine*, vol. 22, nº 2, pp. 8-20, 2002, doi: 10.1109/37.993309
[Sánchez M., 2015]	Sánchez M. Antonio M., «Un modelo general de referencia para el acceso remoto a laboratorios docentes y de investigación» Universidad de Huelva, 2015. https://dialnet.unirioja.es/servlet/tesis?codigo=46908
[Sarno C., 2016]	Sarno C., A. Garofalo, I. Matteucci, M. Vallini, « A novel security information and event management system for enhancing cyber security in a hydroelectric dam», International Journal of Critical Infrastructure Protection 13 (2016).
[Sarker E., 2021]	Sarker E. *et al.*, «Progress on the demand side management in smart grid and optimization approaches», *International Journal of Energy Research*, vol. 45, nº 1, pp. 36-64, 2021, doi: https://doi.org/10.1002/er.5631
[Sembiring Z., 2020]	Sembiring Z., «Stuxnet Threat Analysis in SCADA (Supervisory Control And Data Acquisition) and PLC (Programmable Logic Controller) Systems», *Journal of Computer Science, Information Technology and Telecommunication Engineering*, vol. 1, nº 2, Art. nº 2, 2020, doi: 10.30596/jcositte.v1i2.5116
[Setola R., 2016]	Setola R., V. Rosato, E. Kyriakides, E. Rome, Managing the Complexity of Critical Infrastructures a Modelling and Simulation Approach, Studies in Systems, Decision and Control 90 (2016).
[Shrestha M., 2020]	Shrestha M., Johansen C., Noll J., y Roverso D., «A Methodology for Security Classification applied to Smart Grid Infrastructures», *International Journal of Critical Infrastructure Protection*, vol. 28, p. 100342, mar. 2020, doi: 10.1016/j.ijcip.2020.100342
[SIEMENS, 2014]	SIEMENS, Advance The magazine for Totally Integrated Automation, Núm1, April 2014. https://assets.new.siemens.com/siemens/assets/api/ uuid:7414ea58057a1731bb917c22b4ebffd1956ef3b0/version:1542790198/ advance- 2014- 1- en.pdf, 2014

[SIEMENS, 2016]	SIEMENS Security Advisory, Computer Emergency Response Team CERT, SSA 833048: vulnerability in SIMATIC S7 1200 CPU´s prior to v4, 2016.
[SINEMA R.C., 2020]	SINEMA R.C. (REMOTE CONNECT). (https://w3.siemens.com/mcms/industrial communication/es/industrial- remote-communication/remote- networks/pages/ sinema-remote- connect- access- service.aspx), 2020.
[Snaz A., 2013]	Snaz A., «China, EEUU y las APT: La importancia del informe Mandiant», *INCIBE-CERT*, 2013. https://www.incibe-cert.es/blog/china-eeuu-apt-informe-mandiant
[Stergiopoulss G., 2015]	Stergiopoulss G., P. Kotzanikolaou, M. Theocharidou, G. Lykou, D. G.«Time based critical infrastructure dependency analysis for large scale and cross sectorial failures», International Journal of Critical Infrastructure Protection 12 (2015).
[Stouffer K., 2015]	Stouffer K., Lightman S., Pillitteri V., Abrams M., y Hahn A., «Guide to Industrial Control Systems (ICS) Security», National Institute of Standards and Technology, NIST Special Publication (SP) 800-82 Rev. 2, jun. 2015. doi: https://doi.org/10.6028/NIST.SP.800-82r2
[Stouffer K., 2020]	Stouffer, K., Zimmerman, T., Tang, C., Pease, M., Lubell, J., Cichonski, J., & McCarthy, J. (2020). «*Cybersecurity Framework Version 1.1 Manufacturing Profile* (No. NIST Internal or Interagency Report (NISTIR)» 8183 Rev. 1. National Institute of Standards and Technology.
[Straub J., 2020]	Straub J., «Modeling Attack, Defense and Threat Trees and the Cyber Kill Chain, ATT CK and STRIDE Frameworks as Blackboard Architecture Networks», en *2020 IEEE International Conference on Smart Cloud (SmartCloud)*, nov. 2020, pp.148-153. doi:10.1109/SmartCloud49737.2020.00035
[Tascón S., 2020]	Tascón S. Q., Jiménez J. Z., y Montoya H. F. V., «Predicción de ciberataques en sistemas industriales SCADA a través de la implementación del filtro Kalman», *Tecnológicas*, vol. 23, n.º 48, Art. n.º 48, may 2020, doi: 10.22430/22565337.1586
[Tengfei T., 2017]	Tengfei T., Hua Zhang, Boqin Qin, y Zhuo Chen, «A Vulnerability Mining System Based on Fuzzing for IEC 61850 Protocol», en *Proceedings of the 2017 5th*

	International Conference on Frontiers of Manufacturing Science and Measuring Technology (FMSMT 2017), abr. 2017, pp. 589-597. doi: 10.2991/fmsmt-17.2017.119
[Trend-Micro, 2019]	Trend-Micro, « Security in the Era of Industry 4.0: Dealing With Threats to Smart Manufacturing Environments – Security News» 2019. https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/security-in-the-era-of-industry-4-dealing-with-threats-to-smart-manufacturing-environments
[Tripathi S., 2021]	Tripathi S. y Gupta M., «A holistic model for Global Industry 4.0 readiness assessment», *Benchmarking: An International Journal*, vol. ahead-of-print, n.º ahead-of-print, ene. 2021, doi: 10.1108/BIJ-07-2020-0354
[Tweneboah-Koduah S., 2020]	Tweneboah-Koduah S. y Prasad R., «The Threats of Infrastructure Obsolescence to Smart Grid: A Case Study», *Wireless Pers Commun*, vol. 114, nº 2, pp. 1025-1043, sep. 2020, doi: 10.1007/s11277-020-07406-y
[US CERT, 2016]	US CERT, United States Computer Emergency Readiness, National Cybersecurity and Communications Integration Center (NCCIC) of the Department of Homeland Security, 2016.
[Upadhyay D., 2020]	Upadhyay D., S. Sampalli, «SCADA (Supervisory Control and Data Acquisition) systems: vulnerability assessment and security recommendations», Computer and Security Journal (2020), doi: 10.1016/j.cose.2019.101666
[Ustun T., 2013]	Ustun T. S., Ozansoy C. R., y Zayegh A., «Implementing Vehicle-to-Grid (V2G) Technology With IEC 61850-7-420», *IEEE Transactions on Smart Grid*, vol. 4, nº 2, pp. 1180-1187, jun. 2013, doi: 10.1109/TSG.2012.2227515
[Vargas J., 2020]	Vargas J. Cuero, Universidad de los Llanos, Colombia, C. Torres, y Universidad de los Llanos, Colombia, «Laboratorios Remotos e IOT una oportunidad para la formación en ciencias e ingeniería en tiempos del COVID-19: Caso de Estudio en Ingeniería de Control», *Espacios*, vol. 41, n.º 42, nov. 2020, doi: 10.48082/espacios-a20v41n42p16
[Wang S., 2016]	Wang S., an analytical model for benchmarking the development of national infrastructure items against those in similar countries, International Journal of Critical Infrastructure Protection 13 (2016).

[Warnier M., 2017]	Warnier M., Dulman S., Koç Y., y Pauwels E., «Distributed monitoring for the prevention of cascading failures in operational power grids», *International Journal of Critical Infrastructure Protection*, vol. 17, pp. 15-27, jun. 2017, doi: 10.1016/j.ijcip.2017.03.003
[Xionj J., 2021]	Xiong J., Bu X., Huang Y., Shi J., y He W., «Safety Verification of IEC 61131-3 Structured Text Programs», *IEEE Transactions on Industrial Informatics*, vol. 17, n.º 4, pp. 2632-2640, 2021, doi: 10.1109/TII.2020.2999716
[Yamin M., 2020]	Yamin M., Katt B., y Gkioulos V., «Lab Cyber ranges and security test beds: Scenarios, functions, tools and architecture», *Computers & Security*, vol. 88, p. 101636, 2020, doi: 10.1016/j.cose.2019.101636
[Zafirovic-Vukotic M., 2009]	Zafirovic-Vukotic M., Moore R., Leslie M., Midence R., y Pozzuoli M., «Secure SCADA network supporting NERC CIP», en *2009 IEEE Power Energy Society General Meeting*, jul. 2009, pp. 1-8. doi: 10.1109/PES.2009.5275559
[Zhang M., 2019]	Zhang M. y Li Y., «Students' Continuance Intention to Experience Virtual and Remote Labs in Engineering and Scientific Education», *Int. J. Emerg. Technol. Learn.*, vol. 14, n.º 17, p. 4, 2019, doi: 10.3991/ijet.v14i17.10799
[Zhang Y., 2020]	Zhang Y. *et al.*, «All Your PLCs Belong to Me: ICS Ransomware Is Realistic», en *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, dic. 2020, pp. 502-509. doi: 10.1109/TrustCom50675.2020.00074
[Zurfluh R., 2019]	Zurfluh R., «OT Security – How ICS & IACS infrastructures can be operated securely», 2019. https://www.infoguard.ch/en/blog/ot-security-how-ics-iacs-infrastructures-can-be-operated-securely

Localizadores de recursos

[URL- 00, 2021]	**Repositorio de documentación de la Tesis** **Esa URL corresponde a la ubicación de Google Drive en donde se aloja toda la extensa documentación técnica referenciada y utilizada en la Tesis.** https://drive.google.com/drive/folders/1ESodP_i-gD76cay2U1ddVdS0U1nY7WuP?usp=sharing

[URL- 01, 2021]	http://tesauros.mecd.es/tesauros/contextosculturales/1191477.html
[URL- 02, 2021]	https://curiosfera-historia.com/historia-rueda-origen-inventor-evolucion/
[URL- 03, 2020]	https://yiminshum.com/mobile-movil-app-2020/
[URL-04, 2020]	https://es.statista.com/temas/6976/el-internet-de-las-cosas-iot/
[URL-05, 2015]	https://www.incibe-cert.es/blog/divide-venceras-segmentacion-rescate
[URL-06, 2016]	https://www.uma.es/foroparalapazenelmediterraneo/wp-content/uploads/2017/04/Infraestructuras-Critica-Francisco-J-Galindo-Sierra1.pdf
[URL- 07, 2018]	https://www.incibe-cert.es/blog/amenazas-emergentes-sistemas-control-industrial
[URL- 08, 2015]	https://www.incibe-cert.es/alerta-temprana/bitacora-ciberseguridad/primer-corte-suministro-historia-debido-ciberataque
[URL- 09, 2017]	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
[URL- 10, 2015]	https://www.nist.gov/publications/guide-industrial-control-systems-ics-security
[URL- 11, 2017]	https://www.isa.org/pdfs/autowest/phinneydone/
[URL- 12, 2011]	https://boe.es/buscar/pdf/2011/BOE-A-2011-7630-consolidado.pdf
[URL- 13, 2013]	https://www.incibe-cert.es/blog/china-eeuu-apt-informe-mandiant
[URL- 14, 2021]	https://www.ccn-cert.cni.es/

[URL- 15, 2016]	https://www.incibe.es/sites/default/files/estudios/tendencias_en_el_mercado_de_la_ciberseguridad.pdf
[URL- 16, 2019]	https://blog.infaimon.com/mejora-procesos-optimizacion-los-procesos-ya-existentes/
[URL- 17, 2019]	https://www.incibe-cert.es/blog/el-responsable-ciberseguridad-industrial-actualidad
[URL- 18, 2021]	https://www.shodan.io/
[URL- 19, 2021]	https://www.zoomeye.org/
[URL- 20, 2021]	https://support.industry.siemens.com/cs/document/109771672/versi%C3%B3n-de-firmware-v4-4-liberada-para-el-s7-1200?dti=0&lc=es-ES
[URL- 21, 2021]	https://www.cvedetails.com/vulnerability-list/vendor_id-109/product_id-37876/Siemens-Simatic-S7-1200-Firmware.html
[URL- 22, 2021]	https://www.iso27000.es/iso27002.html
[URL- 23, 2021]	https://www.first.org/cvss/
[URL- 24, 2021]	https://nvd.nist.gov/vuln-metrics/cvss/v2-calculator/
[URL- 25, 2021]	http://www.ciberderecho.com/que-son-las-ciberamenazas/
[URL- 26, 2021]	https://www.incibe-cert.es/blog/insider-las-dos-caras-del-empleado
[URL- 27, 2007]	https://www.muckrock.com/news/archives/2016/nov/14/aurora-generator-test-homeland-security/ *"Proyecto Aurora".*
[URL- 28, 2020]	https://elpais.com/internacional/2020-05-19/iran-e-israel-se-miden-en-una-ciberguerra-soterrada.html
[URL- 29, 2021]	https://us-cert.cisa.gov/ics/advisories/icsa-21-012-05
[URL- 30, 2021]	https://drive.google.com/file/d/1s3Yl3XLbEy8C27XoCluTLZBfEkMOqA6B/view?usp=sharing "*US-CERT Vulnerabilities".*
[URL- 31, 2021]	https://drive.google.com/file/d/1t1dY2ykA8hOSp0UkadoZ9C-W0j_LMRiF/view?usp=sharing *"NIST 800-82 rev2"*
[URL- 32, 2019]	https://www.incibe.es/protege-tu-empresa/blog/dmz-y-te-puede-ayudar-proteger-tu-empresa
[URL- 33, 2017]	http://web.mit.edu/smadnick/www/wp/2017-09.pdf
[URL- 34, 2018]	https://www.nrc.gov/docs/ML0925/ML092540336.pdf
[URL- 35, 2006]	https://www.nrc.gov/docs/ML0634/ML063470173.pdf
[URL- 36, 2008]	https://www.silicon.es/un_chaval_polaco_de_14_anos_hackea_una_red_ferroviaria_-101388
[URL- 37, 2008]	https://www.nrc.gov/docs/ML0903/ML090300122.pdf
[URL- 38, 2021]	https://inl.gov/
[URL- 39, 2007]	https://drive.google.com/file/d/1dUJSFteglJOUlLbTk6ypvGZoC-NRj071/view?usp=sharing

[URL- 40, 2021]	https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/5377-ccn-cert-ia-13-20-ciberamenazas-y-tendencias-edicion-2020/file.html
[URL- 41, 2021]	https://www.sofistic.com/blog-ciberseguridad/tendencias-ciberseguridad-2021/#informe
[URL- 42, 2020]	https://www.fortinet.com/lat/corporate/about-us/newsroom/press-releases/2020/fortiguard-labs-predicts-weaponizing-of-the-intelligent-edge-will-dramatically-alter-speed-and-scale-of-future-cyberattacks
[URL- 43, 2021]	https://ccdcoe.org/exercises/locked-shields/
[URL- 44, 2021]	https://www.ccdcoe.org/library/strategy-and-governance/?category=cyber-security-strategies
[URL- 45, 2021]	https://www.ccn-cert.cni.es/empresas-de-interes-estrategico/marco-normativo.html
[URL- 46, 2021]	https://ec.europa.eu/info/index_en
[URL- 47, 2021]	https://www.enisa.europa.eu/
[URL- 48, 2021]	https://www.dhs.gov/
[URL- 49, 2021]	https://cnnic.com.cn/AU/Introduction/Introduction/201208/t20120815_33295.htm Gobierno Chino
[URL- 50, 2004]	https://www.boe.es/buscar/doc.php?id=BOE-A-2004-5051
[URL- 51, 2007]	https://www.lamoncloa.gob.es/Paginas/archivo/021107-enlacecriticas.aspx
[URL- 52, 2010]	https://www.boe.es/buscar/act.php?id=BOE-A-2010-1330
[URL- 53, 2011]	https://www.boe.es/buscar/doc.php?id=BOE-A-2011-7630 Ley PIC
[URL- 54, 2011]	https://www.boe.es/buscar/doc.php?id=BOE-A-2011-8849 Reglamento PIC
[URL- 55, 2011]	http://www.realinstitutoelcano.org/wps/wcm/connect/c06cac0047612e998806cb6dc6329423/EstrategiaEspanolaDeSeguridad.pdf?MOD=AJPERES&CACHEID=c06cac0047612e998806cb6dc6329423 Estrategia de Seguridad Nacional 2011
[URL- 56, 2013]	https://www.dsn.gob.es/es/estrategias-publicaciones/estrategias/estrategia-seguridad-nacional Estrategia de Seguridad nacional 2013
[URL- 57, 2017]	https://www.boe.es/buscar/doc.php?id=BOE-A-2017-15181 Estrategia de Seguridad nacional 2017
[URL- 58, 2018]	https://www.boe.es/diario_boe/txt.php?id=BOE-A-2018-12257 Ley NIS

[URL- 59, 2019]	https://www.boe.es/eli/es/o/2019/04/26/pci487 Estrategia ciberseguridad 2019
[URL- 60, 2020]	https://www.lamoncloa.gob.es/presidente/actividades/Documents/2020/ENIA2B.pdf. Estrategia nacional inteligencia artificial
[URL- 61, 2020]	https://www.boe.es/buscar/act.php?id=BOE-A-2020-9138 reorganización CNPIC.
[URL- 62, 2021]	https://www.boe.es/diario_boe/txt.php?id=BOE-A-2021-1192 Reglamento NIS.
[URL- 63, 2021]	https://avancedigital.mineco.gob.es/es-es/Participacion/Paginas/DetalleParticipacionPublica.aspx?k=346
[URL- 64, 2016]	https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016L1148 Ley NIS
[URL- 65, 2020]	https://ec.europa.eu/digital-single-market/en/news/eus-cybersecurity-strategy-digital-decade Estrategia ciberseguridad europea
[URL- 66, 2020]	https://ec.europa.eu/digital-single-market/en/cybersecurity-strategy
[URL- 67, 2014]	https://www.congress.gov/bill/113th-congress/senate-bill/2519/text?q=%7b%22search%22:%5b%22cybersecurity%22%5d%7d
[URL- 68, 2015]	https://fas.org/sgp/crs/natsec/R44023.pdf
[URL- 69, 2017]	https://www.congress.gov/bill/115th-congress/senate-bill/770/text
[URL- 70, 2018]	https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf
[URL- 71, 2018]	https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf
[URL- 72, 2020]	https://www.ccdcoe.org/uploads/2018/10/USA_National-Strategy-to-Secure-5G_2020.pdf
[URL- 73, 2016]	https://cnnic.com.cn/AU/Introduction/Introduction/201208/t20120815_33295.htm información gobierno China
[URL- 74, 2014]	https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy/
[URL- 75, 2021]	http://nic.af/Content/files/National%20Cybersecurity%20Strategy%20of%20Afghanistan%20(November2014).pdf Afganistan
[URL- 76, 2021]	http://rustrans.wikidot.com/russia-s-national-security-strategy-to-2020
[URL- 77, 2021]	https://webstore.iec.ch/publication/6028
[URL- 78, 2021]	https://webstore.iec.ch/searchform&q=62443
[URL- 79, 2021]	https://www.iec.ch/energies/smart-energy

[URL- 80, 2021]	https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa99
[URL- 81, 2021]	https://www.nist.gov/
[URL- 81 (a), 2010]	https://scp.nrc.gov/slo/regguide571.pdf
[URL- 82, 2021]	https://www.nerc.com/Pages/default.aspx
[URL- 83, 2021]	https://standards.ieee.org/
[URL- 84, 2021]	https://www.api.org/
[URL- 85, 2021]	https://www.incibe-cert.es/laboratorios
[URL- 86, 2021]	https://www.bcit.ca/
[URL- 87, 2019]	https://towardsdatascience.com/batch-mini-batch-stochastic-gradient-descent-7a62ecba642a
[URL- 88, 2017]	https://www.dsn.gob.es/estrategias-publicaciones/estrategias/estrategia-seguridad-nacional-2017
[URL- 89, 2021]	https://www.honeynet.org/
[URL- 90, 2021]	http://www.honeyd.org/
[URL- 91, 2021]	http://conpot.org/
[URL- 92, 2021]	https://www.honeynet.org/tag/scada-d51/
[URL- 93, 2021]	https://foronacionalciberseguridad.es/
[URL- 94, 2020]	https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/5428-ccn-cert-bp-20-buenas-pra-cticas-en-la-gestio-n-de-cibercrisis-1/file.html
[URL- 95, 2021]	https://www.nbcnews.com/news/us-news/power-comes-back-most-texas-other-problems-pile-n1258311
[URL- 96, 2019]	https://www.boe.es/eli/es/o/2019/04/26/pci487/dof/spa/pdf
[URL- 97, 2021]	https://es.mathworks.com/products/simulink.html
[URL- 98, 2019]	https://www.incibe.es/protege-tu-empresa/blog/importancia-proteger-informacion-mediante-acuerdos-confidencialidad
[URL- 99, 2021]	https://cybersecurity.att.com/blogs/security-essentials/siem-what-is-it-and-why-does-your-business-need-it
[URL- 100, 2021]	https://thestandardcio.com/2020/09/30/que-son-las-maquinas-virtuales/
[URL- 101, 2021]	https://www.virtualbox.org/
[URL- 102, 2021]	https://www.vmware.com/es.html
[URL- 103, 2021]	https://support.industry.siemens.com/cs/document/109744660/%C2%BFqu%C3%A9-escenarios-nat-se-pueden-implementar-con-scalance-sc-600-m-800-s615-?dti=0&lc=es-ES
[URL- 104, 2021]	https://www.icm.es/2019/12/05/tunel-ipsec-openvpn/

[URL- 105, 2021]	https://standards.ieee.org/standard/802_11n-2009.html
[URL- 106, 2021]	https://new.siemens.com/global/en/products/automation/simatic-hmi/panels/comfort-panels.html
[URL- 107, 2021]	https://www.tecnoplc.com/coste-energetico-reducido-40/
[URL- 108, 2021]	https://www.first.org/cvss/
[URL- 109, 2021]	https://www.openvas.org/
[URL- 110, 2021]	https://oval.mitre.org
[URL- 111, 2021]	https://www.first.org/cvss/specification-document
[URL- 112, 2016]	https://nvd.nist.gov/vuln/detail/CVE-2016-2846
[URL- 113, 2016]	https://us-cert.cisa.gov/ics/advisories/ICSA-16-075-01
[URL- 114, 2016]	https://cert-portal.siemens.com/productcert/txt/ssa-833048.txt
[URL- 115, 2020]	https://www.helpnetsecurity.com/2020/12/09/vulnerable-tcp-ip-stacks/
[URL- 116, 2021]	https://www.first.org/cvss/v3.1/user-guide#5-Scoring-Rubrics
[URL- 117, 2021]	https://www.incibe-cert.es/laboratorios
[URL- 118, 2019	https://www.iec.ch/homepage
[URL- 119, 2021]	https://www.incibe-cert.es/blog/estandar-iec-61850-todos-uno-y-uno-todos
[URL- 120, 2021]	https://www.smartgridsinfo.es/2021/03/25/sistema-control-spectrum-power-7-siemens-gestionara-red-electrica-suecia
[URL- 121, 2021]	https://www.omicronenergy.com/es/productos/iedscout/
[URL- 122, 2020]	http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ciberseguridad/ari3-2020-ayerbe-la-ciberseguridad-en-el-sector-energetico
[URL- 123, 2019]	https://www.tendencias.kpmg.es/2019/09/cadena-suministro-digital/
[URL- 124, 2021]	https://www.smart-energy.com/industry-sectors/data_analytics/iot-for-utilities-harnessing-big-data-from-grids-edge/
[URL- 125, 2021]	https://www.incibe-cert.es/alerta-temprana/bitacora-ciberseguridad/interrupcion-el-suministro-del-oleoducto-colonial-pipeline
[URL- 125 (a), 2020]	https://peoplesenergy.co.uk/help/data-incident
[URL- 125 (b), 2020]	https://www.bbc.com/news/technology-55350995
[URL- 125 (c), 2020]	https://www.infosecurity-magazine.com/news/uk-energy-data-breach-customer/

[URL- 126 (a), 2020]	https://sicnoticias.pt/pais/2020-04-13-EDP-alvo-de-ataque-informatico
[URL- 126 (b), 2020]	https://www.bleepingcomputer.com/news/security/ragnarlocker-ransomware-hits-edp-energy-giant-asks-for-10m/
[URL- 126 (c), 2020]	https://www.genbeta.com/seguridad/energetica-edp-sufre-ciberataque-atacantes-piden-rescate-10-millones-medio-portugues
[URL- 126 (d), 2020]	https://cincodias.elpais.com/cincodias/2020/04/14/companias/1586887179_127560.html
[URL- 126 (e), 2020]	https://www.eleconomista.es/energia/noticias/10481205/04/20/EDP-sufre-un-ciberataque-y-le-piden-10-millones-para-liberarla.html
[URL- 126 (f), 2020]	https://www.elespanol.com/omicrono/software/20200506/publican-datos-confidenciales-electrica-edp-despues-millones/487952161_0.html
[URL- 127 (a), 2019]	https://www.pemex.com/saladeprensa/boletines_nacionales/Paginas/2019-47_nacional.aspx
[URL- 127 (b), 2019]	https://elpais.com/economia/2019/11/12/actualidad/1573534824_855018.html
[URL- 127 (c), 2019]	https://www.bloomberg.com/news/articles/2019-11-13/a-hacker-wants-about-5-million-from-pemex-by-end-of-november
[URL- 127 (d), 2019]	https://vanguardia.com.mx/articulo/ataque-cibernetico-pemex-totalmente-controlado-y-sin-consecuencias-alfonso-durazo
[URL- 127 (e), 2019]	https://www.europapress.es/internacional/noticia-petrolera-estatal-pemex-asegura-ataque-cibernetico-completamente-control-20191115042848.html
[URL- 127 (f), 2019]	https://www.xataka.com.mx/seguridad/pemex-podria-estar-trabajando-formatos-papel-supuesto-rescate-al-ataque-tiene-fecha-limite-30-noviembre
[URL- 128 (a), 2019]	https://us-cert.cisa.gov/ncas/current-activity/2019/10/21/nsa-and-ncsc-release-joint-advisory-turla-group-activity
[URL- 128 (b), 2019]	https://www.incibe-cert.es/alerta-temprana/bitacora-ciberseguridad/informe-actividad-del-grupo-turla-elaborado-nsa-y-el-ncsc
[URL- 128 (c), 2019]	https://www.ncsc.gov.uk/news/turla-group-exploits-iran-apt-to-expand-coverage-of-victims
[URL- 128 (d), 2019]	https://www.incibe-cert.es/alerta-temprana/bitacora-ciberseguridad/el-grupo-turla-ataca-nuevo
[URL- 129 (a), 2019]	https://twitter.com/CityPowerJhb/status/1154277777950093313

[URL- 129 (b), 2019]	https://twitter.com/CityofJoburgZA/status/1154314614844399616
[URL- 129 (c), 2019]	https://www.teknofilo.com/la-ciudad-de-johannesburgo-se-queda-sin-luz-debido-a-un-ataque-de-ransomware/
[URL- 129 (d), 2019]	https://www.bbc.com/news/technology-49125853
[URL- 130 (a), 2019]	https://www.fireeye.com/blog/threat-research/2019/04/triton-actor-ttp-profile-custom-attack-tools-detections.html
[URL- 130 (b), 2019]	https://techcrunch.com/2019/04/09/triton-malware-strike/?guccounter=1
[URL- 130 (c), 2019]	https://www.wired.com/story/triton-hacker-toolkit-fireeye/
[URL- 130 (d), 2019]	https://www.csoonline.com/article/3388228/group-behind-triton-industrial-sabotage-malware-made-more-victims.html
[URL- 130 (e), 2019]	http://www.zonavirus.com/noticias/2019/segunda-vez-que-usan-el-malware-triton-para-hacer-estallar-una-planta-petroquimica.asp
[URL- 130 (f), 2019]	https://www.dailymail.co.uk/sciencetech/article-6913775/Experts-warn-hackers-murderous-malware-Triton-targeting-critical-infrastructure.html
[URL- 131 (a), 2018]	https://www.welivesecurity.com/la-es/2018/10/17/greyenergy-actores-maliciosos-peligrosos-arsenal-actualizado/
[URL- 131 (b), 2018]	https://www.cyberscoop.com/greyenergy-eset-ukraine-sandworm-telebots/
[URL- 131 (c), 2018]	https://www.hackread.com/greyenergy-malware-hits-energy-sector-with-espionage/
[URL- 131 (d), 2018]	https://www.elespanol.com/invertia/disruptores-innovadores/innovadores/tecnologicas/20181017/greyenergy-nueva-ciberamenaza-podria-tumbar-sistema-electrico/346216897_0.html
[URL- 132 (a), 2017]	https://community.broadcom.com/symantecenterprise/viewdocument/dragonfly-westliche-energieunterne?CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments
[URL- 132 (b), 2017]	https://arstechnica.com/information-technology/2017/09/hackers-lie-in-wait-after-penetrating-us-and-europe-power-grid-networks/
[URL- 132 (c), 2017]	https://thehackernews.com/2017/09/dragonfly-energy-hacking.html
[URL- 132 (d), 2017]	https://www.incibe-cert.es/alerta-temprana/bitacora-ciberseguridad/apt-sistemas-control-industrial

[URL- 133 (a), 2017]	https://www.theregister.com/2016/12/21/ukraine_electricity_outage/
[URL- 133 (b), 2017]	https://www.incibe-cert.es/blog/nuevo-ciberataque-red-electrica-ucrania
[URL- 133 (c), 2017]	https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/
[URL- 133 (d), 2017]	https://www.wired.com/story/crash-override-malware/
[URL- 133 (e), 2017]	https://eu.usatoday.com/story/tech/news/2017/06/12/malware-discovered-could-threaten-electrical-grid/102775998/
[URL- 133 (f), 2017]	https://dragos.com/blog/crashoverride/CrashOverride-01.pdf
[URL- 134 (a), 2016]	https://arstechnica.com/information-technology/2016/01/israels-electric-grid-hit-by-severe-hack-attack/
[URL- 134 (b), 2016]	https://www.sans.org/blog/?focus-area=industrial-control-systems-security
[URL- 134 (c), 2016]	https://news.softpedia.com/news/israel-s-power-grid-targeted-by-ransomware-499488.shtml
[URL- 135 (a), 2015]	https://www.reuters.com/article/us-ukraine-crisis-malware-idUSKBN0UE0ZZ20151231
[URL- 135 (b), 2015]	https://www.welivesecurity.com/2016/01/04/blackenergy-trojan-strikes-again-attacks-ukrainian-electric-power-industry/
[URL- 135 (c), 2015]	https://arstechnica.com/information-technology/2016/01/first-known-hacker-caused-power-outage-signals-troubling-escalation/
[URL- 135 (d), 2015]	https://elperiodicodelaenergia.com/el-primer-ciberataque-de-la-historia-contra-una-electrica-pone-en-alerta-a-todo-el-sector/
[URL- 135 (e), 2015]	https://edition.cnn.com/2016/02/11/politics/ukraine-power-grid-attack-russia-us/
[URL- 135 (f), 2015]	https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/
[URL- 136 (a), 2015]	https://money.cnn.com/2015/10/15/technology/isis-energy-grid/index.html
[URL- 136 (b), 2015]	https://www.businessinsider.com/isis-and-hacking-us-power-grid-2015-10?IR=T
[URL- 136 (c), 2015]	https://www.israel365news.com/51687/homeland-security-reveals-isis-attempted-to-sabotage-power-grid-through-cyber-attacks-terror-watch/#FeKbr4y2lLGwi8jO.97
[URL- 137, 2021]	https://www.incibe-cert.es/blog/control-peticiones-multicast-el-estandar-iec-61850

[URL- 138, 2021]	https://www.une.org/encuentra-tu-norma/busca-tu-norma/proyecto?c=P0050868
[URL- 139, 2021]	https://www.omicronenergy.com/es/productos/iedscout/
[URL- 140, 2021]	https://wiki.wireshark.org/IsoProtocolFamily
[URL- 141, 2021]	https://www.incibe.es/protege-tu-empresa/blog/el-ataque-del-man-middle-empresa-riesgos-y-formas-evitarlo
[URL- 142, 2020]	https://global.abb/group/en
[URL- 143, 2021]	https://www.arcteq.fi/

Anexos

Anexo I:

Otros méritos.

A lo largo del tiempo discurrido para la materialización de esta Tesis Doctoral, se han podio llevar a cabo una diversidad de actividades (directa e indirectamente relacionadas con el núcleo principal de la Tesis).

- ***Colaboración como investigador CCDCoE- OTAN***.

Durante un periodo de tres meses, se materializó una colaboración como investigador en materia de ciberseguridad en dispositivos industriales adscritos al sector eléctrico (ramas de generación y transporte energético), en el proyecto “"ICS Vulnerability Research and Pentesting". La investigación se desarrolló en el Centro de Ciber-Excelencia Cooperativa de la OTAN (Tallin-Estonia).

- ***Ciber-maniobras militares OTAN LockedShield 2014-2019, en el Mando Conjunto del Ciberespacio (MCCE).***

Participación como Team Leader Critical Infrastructure Protecction, ciber-ejercicios OTAN LockedShield 2014-2019, como miembro del equipo español de protección de los sistemas de control industrial de las infraestructuras críticas desplegadas en el entorno de maniobras.

- ***Formación internacional en el US-CERT Idaho Falls (EEUU).***

Realización de curso de formación y especialización en pentesting de sistemas SCADA y redes industriales de infraestructuras críticas, (Idaho Falls, estado de Idaho, Estados Unidos de América).

- ***Formación internacional ATIX (Attack the Network Interagency Exploitation and Analysis” Centro de Excelencia contra Explosivos de la OTAN (España).***

Curso recibido por parte de varias agencias internacionales de inteligencia de Estados Unidos de América y servicios policiales europeos.

Asistencia II Congreso internacional ciberseguridad en Sibiu (Rumania) "CyberSecurity a Central European Public-Private Dialogue Platform".

- ***Director adjunto curso "Experto Universitario, Ciberseguridad en Sistemas de Control Industrial ICS / SCADA". Universidad Nacional de Educación a Distancia (2014-2021)[129].***
- ***Impartición de Talleres técnicos y ponencias técnicas impartidas.***
    - *Taller práctico-técnico CiberWall 2019[130].* "Vulnerabilidades en sistemas de control industrial".
    - *Taller práctico-técnico CiberLeague 2019.[131]* "Ciberataques en sistemas de control industrial - prevención defensa - resiliencia".
    - *Ponente en las IV-V-VI-VII, Jornadas Sobre Tecnología y Nuevas Emergencias"* I+D+e Investigación y Desarrollo Aplicada a la Gestión de la Emergencia.
    - *Ponente en Master Universitario* en Protección de datos Transparencia y Acceso a la Información de la Universidad San Pablo CEU.
    - *Ponencias impartidas (2013-2020) en materia de ciberseguridad de infraestructuras críticas adscritas y sectores estratégicos-críticos nacionales (Centro Nacional para la Protección de Infraestructuras Críticas y Ciberseguridad, CNPIC[132]).*

[129] https://formacionpermanente.uned.es/tp_actividad/idactividad/11938

[130] https://c1b3rwallacademy.usal.es/

[131] https://www.nationalcyberleague.es/

[132] https://www.csirt.es/index.php/es/miembros/cnpic

- Ponencia impartida en empresa auditora en el área de las TIC, Accenture, "Ciberseguridad e informática forense", Universidad Autónoma de Madrid.

- ***Publicaciones oficiales en revistas científicas***.
  - Publicación de artículo científico, Manuscript Number: IJCIP-2019-76R2 "Obtaining High Preventive and Resilience Capacities in Critical Infrastructure by Industrial Automation Cells", International Journal of Critical Infrastructure Protection[133].
  - Publicación artículo científico "Sistemas de Conocimiento por Experimentación Real Mediante Células de Automatización Industrial". Publicación artículo científico en El Comité Español de Automática (CEA), miembro nacional de la Federación Internacional de Control Automático (IFAC)[134].
  - Publicación de artículo científico en R.I.S. (Revista internacional de Sistemas)[135]. "La teoría general de sistemas como herramienta de investigación y solución ante la ciberseguridad en sistemas de automatización industrial".
  - ***Programas de emisión televisiva y radiofónica.***
  - El Cazador de cerebros RTVE, "Ciberataques. La delincuencia digital[136]".

[133] https://www.sciencedirect.com/science/article/pii/S1874548220300196

[134] https://www.ifac.org/

[135] https://ojs.uv.es/index.php/ris/article/view/14105

[136]https://www.rtve.es/play/videos/el-cazador-de-cerebros/cazador-cerebros-ciberataques-delincuencia-digital/5417722/

- Canal UNED, diversos programas radiofónicos de divulgación y conocimiento en material de ciberseguridad (Tecnologías de la Información y Tecnologías de la Operación).[137]
- Canal UNED, Ciberseguridad en sistemas de control industrial ICS/ SCADA [138].

[137] https://canal.uned.es/video/5c18bd3ab1111f5f718be31b

[138] https://canal.uned.es/video/5a6f92a0b1111fa7168b45b2

Anexo II:

Vulnerabilidades SACI (por fabricante).

Esta sección muestra una compilación de vulnerabilidades de dispositivos industriales agrupadas por fabricante. Su recopilación comprende todas aquellas vulnerabilidades datadas desde el *10 de marzo de 2010 hasta 27 de enero de 2021*. Datos obrantes en el US-CERT, Cybersecurity and Infrastructure Security Agency[139].

Accediendo a cada vulnerabilidad se obtiene la siguiente información:

- *Resumen de la vulnerabilidad.*
- *Productos afectados.*
- *Antecedentes existentes de la vulnerabilidad.*
- *Caracterización de la vulnerabilidad.*
- *Detalles de la vulnerabilidad.*
- *Mitigación*.

El archivo completo, conteniendo un total de 1.573 vulnerabilidades correspondientes a 374 fabricantes diferentes.

[URL- 00, 2021]

https://drive.google.com/drive/folders/1ESodP_i-gD76cay2U1ddVdS0U1nY7WuP?usp=sharing

[139] US-CERT, https://us-cert.cisa.gov/ics/advisories

Anexo III:

Resumen ciber-ataques al sector eléctrico.

1. La distribuidora de energía británica, People´s Energy, sufre una brecha de seguridad. (17-12-2020).	
La distribuidora británica de energía, People's Energy, ha notificado un acceso no autorizado por parte de un tercero a su infraestructura TI, debido a una brecha de seguridad. El incidente fue detectado el 16 de diciembre y ha afectado a una base de datos que almacenaba información personal, salvo aquella de tipo financiero, de clientes actuales y antiguos. La información comprometida abarca: nombres, direcciones, teléfonos, correos, fechas de nacimiento, detalles de tarifas y números de identificación de los contadores de gas y electricidad.	
Referencias: peopleenergy.co.uk (a) - bbc.com (b) - Infosecurity- magazine.com (c)	URL- 125 (a) URL- 125 (b) URL- 125 (c).
2. La energética EDP afectada por el ransomware RagnarLocker (13-04-2020).	
EDP (Energías de Portugal), uno de los principales grupos eléctricos de Europa y el mayor de Portugal, ha sido víctima de un incidente tipo *ransomware*, concretamente el denominado RagnarLocker. Los ciberdelincuentes responsables del ataque publicaron una petición de rescate en la que demandaban 1.580 *bitcoins* (cerca de 10 millones de euros) y aseguraban que extrajeron 10 terabytes de información confidencial de los servidores del grupo empresarial.	
Referencias: sicnoticias.pt (a) - bleepingcomputer.com (b) - genbeta.com (c) cincodias.elpais.com (d) - eleconomista.es (e) - elespanol.com (f)	URL- 126 (a) URL- 126 (b) URL- 126 (c) URL- 126 (d) URL- 126 (e) URL- 126 (f)
3. Petrolera Pemex sufrió ciberataque de ransomware (11-11-2019).	
La compañía mexicana de petróleos Pemex ha admitido, en un comunicado oficial, que fue víctima de un ciberataque el pasado 10 de noviembre. En dicho comunicado, la empresa especificó que el ataque afectó al funcionamiento de menos del 5% de sus equipos y que la producción, abastecimiento e inventarios de combustible estuvieron garantizados.El ciberatacante responsable del *ransomware* exigió el pago de 565 bitcoins, equivalente a unos 5 millones de dólares, como rescate de los equipos cifrados, y estableció la fecha límite para dicho pago en el 30 de noviembre, aunque Rocío Nahle, secretaria de Energía, comunicó que Pemex no pagará el rescate.	
Referencias: pemex.com (a) - elpais.com (b) - bloomberg.com (c) - vanguardia.com.mx (d) - europapress.es (e) -xataka.com.mx (f)	URL- 127 (a) URL- 127 (b)

	URL- 127 (c) URL- 127 (d) URL- 127 (e) URL- 127 (f)

4. Actividad del grupo Turla elaborado por la NSA y el NCSC (21-10-2019).

La NSA (*National Security Agency*) de Estados Unidos y el NCSC (*National Cyber Security Centre*) de Reino Unido han publicado un aviso conjunto sobre la APT (*Advanced Persistent Threat*) del grupo Turla, también conocido como Snake, Uroburos, VENEMOUS BEAR, o Waterbug. El aviso proporciona una actualización del informe del NCSC publicado en enero de 2018 sobre el uso, por parte de Turla, de las herramientas maliciosas Neuron, Nautilus y Snake para robar datos confidenciales. Además, el comunicado afirma que Turla ha comprometido, y actualmente está explotando, la infraestructura y los recursos de un grupo iraní de APT 34, que incluyen las herramientas de Neuron y Nautilus. Según Symantec, APT 34 también son conocidos con los sobrenombres de HELIX, KITTEN y OilRig.

Referencias: *us*-cert.gov (a) - media.defense.gov (b) - ncsc.gov.uk (c) - incibe-cert.es (d)	URL- 128 (a) URL- 128 (b) URL- 128 (c) URL- 128 (d)

5. Johannesburgo víctima de ciberataque de ransomware (24-07-2019).

Johannesburgo, la mayor ciudad de Sudáfrica, se ha visto afectada por un ciberataque de ransomware que ha infectado a un proveedor de electricidad y, en consecuencia, ha dejado a algunos de sus residentes sin luz. La infección afectó a City Power, empresa que suministra energía eléctrica de prepago a los residentes de Johannesburgo y a empresas locales, y que ha reconocido que fue víctima del ciberataque. La base de datos de la empresa, la red interna, las aplicaciones web y el sitio web oficial fueron cifrados por el malware, lo que interrumpió sus operaciones y dejó a sus clientes, más de un cuarto de millón, sin servicio. La ciudad, propietaria de la compañía de electricidad, ha comunicado que la mayoría de los sistemas afectados han sido reparados y puestos de nuevo en funcionamiento, y que actualizarán la información según se la vaya proporcionando el proveedor.

Referencias*: twitter.com (a) - twitter.com (b) - teknofilo.com – (c) bbc.com (d)*	URL- 129 (a) URL- 129 (b) URL- 129 (c) URL- 129 (d)

6. El malware Triton compromete de nuevo una infraestructura crítica (10-04-2019).

Expertos en ciberseguridad de la firma FireEye han publicado un informe explicando que el malware Triton ha sido utilizado de nuevo, después del ataque de 2017, para comprometer una instalación de infraestructura crítica, aún no revelada. La amenaza está diseñada para explorar las redes del objetivo y sabotear sus sistemas de control industrial, a menudo utilizados en centrales eléctricas y refinerías de petróleo y, de esta manera, obtener control en las operaciones de la instalación. Además, la investigación señala que el malware llevaba latente alrededor de un año, durante el cual había estado estudiando la configuración de la red y cómo pivotar de un sistema a otro antes de lanzar el ataque.

Referencias: *fireeye.com (a) - techcrunch.com (b) - wired.com (c) csoonline.com (d) - zonavirus.com (e) - dailymail.co.uk (f)*	URL- 130 (a) URL- 130 (b) URL- 130 (c) URL- 130 (d) URL- 130 (e) URL- 130 (f)

7. Malware GreyEnergy amenaza IC desde 2015 (17-10-2018).

Los investigadores de ESET Anton Cherepanov y Robert Lipovsky han publicado un estudio en el que se revelan detalles de un nuevo actor malicioso apodado GreyEnergy, quien al parecer es el sucesor de BlackEnergy. El primer ataque de este grupo lo habría registrado una compañía eléctrica de Polonia a finales de 2015, pero la mayoría de ciberataques se han concentrado en Ucrania, al igual que ocurrió con BlackEnergy. Además del sector eléctrico, otras infraestructuras críticas, como el transporte público, se habrían visto afectadas. La ciberamenaza combina elementos no sólo de BlackEnergy, sino también de Industroyer. Además, se han encontrado conexiones con ataques a objetivos industriales, como los sistemas SCADA, así como el robo de certificados a un fabricante taiwanés de hardware industrial e IoT denominado Advantech.

Referencias: *welivesecurity.com (a) - cyberscoop.com (b) - hackread.com (c) - elespanol.com (d)*	URL- 131 (a) URL- 131 (b) URL- 131 (c) URL- 131 (d)

8. Dragonfly 2.0: nueva campaña de intrusión en sector eléctrico (06-09-2017).

Una nueva campaña conocida como Dragonfly 2.0 está atacando con el objetivo de infiltrarse en infraestructuras del sector energético en Turquía, Suiza y Estados Unidos. La empresa de seguridad Symantec ha dado a conocer esta nueva versión de Dragonfly como ya ocurriera anteriormente, informando que esta nueva oleada lleva operativa desde diciembre de 2015. En esta campaña los atacantes están utilizando diferentes vectores para lograr acceso a las empresas del sector energético como por ejemplo emails maliciosos con los que realizan intentos de phishing o en los que adjuntar archivos que contienen troyanos. Además, se valen de "backdoors" instaladas previamente para tener acceso directo a los sistemas afectados, además de otros "toolkits" para gestionarlos.

Referencias: *symantec.com (a) - arstechnica.com (b) - thehackernews.com (c) - certsi.es (d)*	URL- 132 (a)

	URL- 132 (b) URL- 132 (c) URL- 132 (d)

9. CrashOverride, el malware que saboteó el suministro eléctrico (12-06-2017).

Una nueva campaña conocida como Dragonfly 2.0 está atacando con el objetivo de infiltrarse en infraestructuras del sector energético en Turquía, Suiza y Estados Unidos. La empresa de seguridad Symantec ha dado a conocer esta nueva versión de Dragonfly como ya ocurriera anteriormente, informando que esta nueva oleada lleva operativa desde diciembre de 2015. En esta campaña los atacantes están utilizando diferentes vectores para lograr acceso a las empresas del sector energético como por ejemplo emails maliciosos con los que realizan intentos de phishing o en los que adjuntar archivos que contienen troyanos. Además, se valen de "backdoors" instaladas previamente para tener acceso directo a los sistemas afectados, además de otros "toolkits" para gestionarlos.

Referencias: *heregister.co.uk (a) - certsi.es (b) - welivesecurity.com (c) - wired.com (d) - usatoday.com (e) - dragos.com (f)*	URL- 133 (a) URL- 133 (b) URL- 133 (c) URL- 133 (d) URL- 133 (e) URL- 133 (f)

10. Ransomware afecta la distribución eléctrica en Israel (25-01-2016).

Un ransomware, distribuido a través de una campaña de phishing, logró colarse en la infraestructura de la Electricity Authority de Israel. La infección se detectó el lunes 25 de enero, día en el que para atajarla tuvieron que desconectar partes de la red eléctrica del país. No se han identificado responsables de este ciberataque.

Referencias: *arstechnica.com (a) - ics.sans.org (b) - news.softpedia.com (c)*	URL- 134 (a) URL- 134 (b) URL- 134 (c)

11. Primer corte de suministro eléctrico de la historia debido a un ciberataque (23-12-2015).

El 23 de diciembre del 2015, la red eléctrica nacional de Ucrania sufrió un ataque informático que provocó un corte de suministro durante varias horas, el cual afectó a más de 600.000 hogares de la región de Ivano-Frankivsk. El ataque se habría realizado mediante el uso del troyano BlackEnergy y de técnicas de ingeniería social. Sería la primera vez en la historia que un ataque informático ha sido capaz de provocar un corte de suministro eléctrico.

Referencias: *reuters.com (a) - welivesecurity.com (b) - arstechnica.com (c) - elperiodicodelaenergia.com (d) - edition.cnn.com (e) - wired.com (f)*	URL- 135 (a) URL- 135 (b) URL- 135 (c)

	URL- 135 (d) URL- 135 (e) URL- 135 (f)

12. ISIS ataca la red de energía de EE.UU. (16-10-2015).

Según funcionarios del gobierno de los Estados Unidos, el Estado Islámico (ISIS) está realizando ciberataques contra compañías eléctricas estadounidenses, aunque ninguno ha tenido éxito. Esta información fue revelada el pasado 14 de octubre en una conferencia en la que participaban empresas del ámbito energético estadounidense. Según informa el FBI, las herramientas usadas para atacar estos sistemas no son lo suficientemente eficaces como para suponer un problema para la seguridad de las compañías, siendo improbable que un ataque sea capaz de inhabilitar todo el sistema energético según indicó John Riggi, jefe de "FBI's cyber division".

Referencias: *money.cnn.com (a) - uk.businessinsider.com (b) - breakingisraelnews.com (c)*	URL- 136 (a) URL- 136 (b) URL- 136 (c)

Anexo IV:

Repositorio documentación extra.

Para poder alojar la documentación extra generada en la confección de esta Tesis Doctoral, se ha habilitado un repositorio de documentación el cual contiene la siguiente estructura de directorios:

- ***C-01- Ficheros _.pcap_snifer_de_red***
  - 01_IED_connect_disconnect_refused_conection_mms.pcapng.
  - 02_IED´s_connent_disconenct.pcapng
- ***C-02- Manuales_técnicos_instrumentación_industrial_CAI***
  - *01_Logo_Power_system_manual.pdf*
  - *02_PLC_S71200_sysetem_manual.pdf*
  - *03_SCALANCE_S615_system_manual.pdf*
  - *04_SCALANCE_S615_system_manual.pdf*
  - *05_SCALANCE_W778_W738_system_manual.pdf*
  - *06_SIMATIC_HMI_Confort_Panels.pdf*
- ***C-03- Ficheros .icd***
  - *01_BT10_IED.icd*
  - *02_BT15_I.icd*
- ***C-04- Normativa***
  - *01_CCDCOE, recopilación leyes españolas ciberseguridad.pdf*
  - *02_Cuadernos estratégicos ciberseguridad_185.pdf*
  - *03_Cybersecurity programs nuclear area egguide571.pdf*
  - *04_Estrategia Nacional Ciberseguridad 2019*
  - *05_Europa 2030*

- *06_NIST 1-1 y C2M2-Evaluacion-ciberseguridad-de-entornos-industriales.pdf*
- *07_NIST.SP.800-82r2.pdf*
- *08_OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf*
- *09_Orden PCI:487:2019, de 26 de abril.pdf*
- *10_Reglamento NIST 2021.pdf*
- *11_Reglamento Protección IC España.pdf*
- *12_Reglamento Decreto Ley Seguridad redes y sistemas información.pdf*

- ***C-05- Guías Buenas Prácticas***
  - *01_CCN_CERT_Buenas Prácticas Gestión Cibercrisis.pdf*
  - *02_Homeland_Security_RP_Patch_Management_S508.pdf*
  - *03_INCIBE_CERT_guia_inventario_de_activos_2020_v1.pdf*
  - *04_INCIBE_CERT_guía_acceso_seguro_dispositivos_campo.pdf*
- ***C-06- Anexos***
  - *01_Resumen_ataques_sector_eléctrico.pdf*
  - *02_Vulnerabilidades_por_fabricante_20210127.pdf*
- ***C-07 Varios documentos, proyectos y informes análisis***
  - *01_Catálogo_empresas_Ciberseguridad_2016.pdf*
  - *02_IEC_61850_8_1_GOOSE_Protocol.pdf*
  - *03_IEDScout_software.pdf*
  - *04_IEDScout_v5_maual.pdf*
  - *05_NIST_SP_800_82r2-pdf*
  - *06_Documentación_desclasificada_ProyectoAurora.zip*

- *07_STUXNET_análisis_exhaustivo_informe_completo.pdf*
- *08_Una_década_de_vulnerabilidades_ICS_2020_Guia_CCI.pdf*
- *09_Vulnerabilidades_por Fabricante.20210127.pdf*
- *10_Script_PLC_From_Zoomeye.pdf*

[URL-00, 2021]

https://drive.google.com/drive/folders/1ESodP_i-gD76cay2U1ddVdS0U1nY7WuP?usp=sharing