Trabajo Fin de Máster
Ingeniería de Telecomunicación

Plan Director de Ciberseguridad Industrial: Aplicación a una Subestación Eléctrica.

Autor: Roberto Lama Rodríguez
Tutor: Alejandro Carballar Rincón

Departamento de Ingeniería Electrónica
Escuela Técnica Superior de Ingeniería
Universidad de Sevilla

Sevilla, 2024

Trabajo Fin de Máster
Ingeniería de Telecomunicación

Plan Director de Ciberseguridad Industrial: Aplicación a una Subestación Eléctrica.

Autor:
Roberto Lama Rodríguez
Tutor:
Alejandro Carballar Rincón
Catedrático de Universidad

Dpto. de Ingeniería Electrónica
Escuela Técnica Superior de Ingeniería
Universidad de Sevilla
Sevilla, 2024

Trabajo Fin de Master: Plan Director de Ciberseguridad Industrial: Aplicación a una Subestación Eléctrica.

Autor: Roberto Lama Rodríguez

Tutor: Alejandro Carballar Rincón

El tribunal nombrado para juzgar el Proyecto arriba indicado, compuesto por los siguientes miembros:
Presidente:

Vocales:

Secretario:

Acuerdan otorgarle la calificación de:

Sevilla, 2024

El Secretario del Tribunal

Agradecimientos

Agradecer a mis padres por hacer posible que haya llegado hasta aquí y por creer en mí hasta en los momentos más difíciles. A mi hermana, por su compañía y apoyo. Muchas gracias a mi tutor, por su implicación, apoyo incondicional y orientación durante la realización de este trabajo.

Roberto Lama Rodríguez
Sevilla, 2024

Resumen

Este proyecto tiene como objetivo principal analizar el estado actual de la ciberseguridad en entornos industriales, para establecer las pautas de diseño de un Plan Director de Ciberseguridad Industrial, con aplicación a Subestaciones Eléctricas. Para ello, se estudiará la situación actual, acotando el alcance e identificando el sistema en consideración. A continuación, se hará un análisis de riesgos considerando distintos escenarios, y se establecerán una serie de medidas para mitigarlos. Se priorizarán cada una de las iniciativas en función del coste temporal y de los riesgos que pretenden mitigar.

Posteriormente, se explorarán las soluciones disponibles, tanto comerciales como de código abierto, en el ámbito de los sistemas de detección de intrusiones (IDS – Intrusion Detection System) y sistemas gestores de eventos de seguridad (SIEM - Security Information and Event Management). Estos sistemas desempeñan un papel crucial en la protección de las infraestructuras críticas de la industria, ante posibles amenazas cibernéticas y formarán parte de las medidas que se proponen en el Plan Director de Ciberseguridad.

Finalmente, se desarrollará un escenario que emule de manera precisa el sistema de control de una subestación eléctrica. Dentro de este entorno simulado, se llevarán a cabo diversos ataques basados en la matriz MITRE ATT&CK, que representa una amplia gama de técnicas utilizadas por ciberdelincuentes. Estos ataques servirán como punto de referencia para evaluar la efectividad de los IDS estudiados.

El trabajo se inscribe en la búsqueda constante de soluciones avanzadas para salvaguardar la infraestructura industrial, promoviendo así la seguridad y la continuidad de los procesos esenciales en un mundo cada vez más digitalizado y expuesto a amenazas cibernéticas.

Abstract

The main objective of this project is to analyze the current state of cybersecurity in industrial environments in order to establish the guidelines for the design of an Industrial Cybersecurity Master Plan, with application to Electrical Substations. For this purpose, the current situation will be studied, delimiting the scope and identifying the system under consideration. Then, a risk analysis will be made considering different scenarios, and a series of measures to mitigate them will be established. Each of the initiatives will be prioritized according to the time cost and the risks they are intended to mitigate.

Subsequently, the available solutions, both commercial and open source, in the field of intrusion detection systems (IDS) and security event management systems (SIEM) will be explored. These systems play a crucial role in protecting critical industry infrastructures from potential cyber threats and will form part of one of the measures proposed in the Cybersecurity Master Plan.

Finally, a scenario will be developed that accurately emulates the control system of an electrical substation. Within this simulated environment, various attacks will be carried out based on the MITRE ATT&CK matrix, which represents a wide range of techniques used by cybercriminals. These attacks will serve as a benchmark to evaluate the effectiveness of the studied IDSs.

The work is part of the ongoing search for advanced solutions to safeguard industrial infrastructure, thus promoting the security and continuity of essential processes in a world that is increasingly digitized and exposed to cyber threats.

Índice

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

Definiciones

- **Activos**: Recursos vinculados con las actividades de operación o de información de la organización.
- **ADU**: Application Data Unit.
- **Amenaza**: Cualquier peligro potencial o evento dañino que pueda explotar una vulnerabilidad y causar daño a un sistema, organización o individuo [1].
- **CCAA** (Controles de Acceso): Sistemas de seguridad, para llevar el control de quién entra en un espacio físico.
- **CCTV** (Circuito Cerrado de Televisión): Sistema de videovigilancia.
- **CIAS** (Confidentiality, Integrity, Availability and Safety): Confidencialidad, Integridad, Disponibilidad y Seguridad, se trata de una manera de modelar amenazas cibernéticas en entornos industriales.
- **Conducto**: Agrupación lógica de los canales de comunicación que conectan dos o más zonas que comparten requisitos de seguridad comunes [2].
- **DCS** (Distributed Control Systems): Sistemas de Control Distribuido. Las funciones de adquisición y control son realizadas por un conjunto de microprocesadores distribuidos cerca de los dispositivos controlados o de los instrumentos monitorizados.
- **DMZ** (Demilitarized Zone): Zona Desmilitarizada.
- **DNS** (Domain Name System): Sistema de Nombres de Dominio.
- **ER**: Escenario de Riesgo.
- **FR** (Fundamental Requirements): Requisitos Fundamentales.
- **Gusano informático**: Programa informático que puede ejecutarse de forma independiente, puede propagar una versión completa de sí mismo a otros hosts de una red y puede consumir recursos informáticos de forma destructiva.
- **Historian**: Es un servicio de software de bases de datos para Control permanente y a largo plazo. Es un componente fundamental del sistema SCADA donde se almacenan logs e informes de los datos históricos de la planta.
- **HMI**: Interfaz hombre-máquina. Permite al operador monitorizar los datos y controlar acciones mediante una pantalla táctil.
- **IACS** (Industrial Automation and Control System): Sistema de Automatización y Control Industrial.
- **IDS** (Intrusion Detection System): Sistema de Detección de Intrusiones. Se encarga de detectar accesos no autorizados en una red.
- **IoT** (Internet of Things): Internet de las cosas.
- **IPS** (Intrusion Prevention System): Sistema de Prevención de Intrusiones.
- **IT** (Information Technology): Tecnologías de la Información.
- **Malware**: Programa que se inserta de forma encubierta en otro programa con la intención de destruir

datos, ejecutar programas destructivos o intrusivos, o comprometer de otro modo la confidencialidad, integridad o disponibilidad de los datos, aplicaciones o sistema operativo de la víctima.

- **Matriz MITRE**: Matriz de seguimiento de incidentes de ciberseguridad detectados en entornos industriales.
- **MBAP**: MODBUS Application Protocol Header.
- **ML**: Niveles de Madurez.
- **Modelo OSI** (Open Systems Interconnection): Marco de trabajo conceptual que define cómo se comunican los sistemas de redes y cómo se envían datos de un remitente a un destinatario. Se usa para describir los componentes de la comunicación de datos, para poder establecer reglas y estándares acerca de las aplicaciones y la infraestructura de red. Contiene siete capas que se apilan (conceptualmente) de abajo a arriba: física, enlace de datos, red, transporte, sesión, presentación y aplicación [3].
- **MR**: Medida de Mitigación de Riesgos.
- **MTU**: Sistema de supervisión. Se trata de un ordenador que recopila los datos del proceso mediante RTUs y permite enviar comandos.
- **OT** (Operational Technology): Tecnología Operativa.
- **PDS**: Plan Director de Seguridad.
- **PDU**: Protocol Data Unit.
- **PLC** (Programmable Logic Controller): Sistema encargado para automatizar procesos electromecánicos, electroneumáticos, electrohidráulicos industriales.
- **RTU** (Remote Terminal Units): Unidades Terminales Remotas. Microprocesadores que obtienen señales de sensores para procesarlas remotamente.
- **SCADA** (Supervisory Control And Data Acquisition): Se encarga de obtener y controlar procesos industriales a distancia.
- **SIEM** (Security Information and Event Management): Gestor de eventos e información de seguridad. Almacena y procesa datos relevantes de seguridad de la red.
- **SIRP** (Security Incident Response Planning): Plan de Respuestas a Incidentes de Seguridad.
- **SL**: Niveles de Seguridad.
- **SOC** (Security Operation Center): Un centro de operaciones de seguridad es un equipo interno o externo de profesionales de la seguridad informática que supervisa toda la infraestructura informática de una organización, 24 horas al día, 7 días a la semana, para detectar incidentes de ciberseguridad en tiempo real y resolverlos con la mayor rapidez y eficacia posibles [4].
- **SR**: Requisitos individuales del sistema de control.
- **SUC** (System Under Consideration): Sistema en consideración.
- **Táctica**: Método utilizado para alcanzar un objetivo específico.
- **Técnica**: Define la forma de realizar acciones o estrategias concretas para alcanzar diferentes objetivos definidos dentro de cada táctica.
- **Vulnerabilidad**: Defecto o debilidad en el diseño, la implementación o el funcionamiento y la gestión de un activo que podría ser explotado por una amenaza.
- **ZCR** (Zone and Conduit Requirement): Requisito de zonas y conductos.
- **Zona**: Agrupación de activos lógicos o físicos basada en el riesgo u otros criterios, como la criticidad de los activos, la función operativa, la ubicación física o lógica, el acceso requerido (por ejemplo, los principios de privilegio mínimo) o la organización responsable.

1 INTRODUCCIÓN

En un mundo cada vez más interconectado y automatizado, la seguridad de los Sistemas de Control y Automatización Industrial (IACS – Industrial Automation and Control System) se han convertido en una preocupación primordial. La Ingeniería de Telecomunicación desempeña un papel crucial en el diseño y mantenimiento de sistemas de comunicación confiables para entornos industriales.

La infraestructura crítica, se considera toda aquella que ofrezca servicios que una sociedad requiere para su correcto funcionamiento, como el suministro de agua, energía, transporte, telecomunicaciones, sistema bancario o sistema de salud. El sector energético es uno de los más afectados por los ciberataques, y esta tendencia ha ido en aumento en los últimos años. Dado que se trata de un sector con información delicada, los ataques pueden tener consecuencias significativas, tanto desde una perspectiva económica como social [5]. En el apartado "1.2 Incidentes de Ciberseguridad Industrial", se comentarán casos en los que se ha visto comprometida la seguridad de IACS, y concretamente de suministro energético.

1.1 Objetivos

1.1.1 Objetivos generales

Establecer las pautas de diseño de un Plan Director de Ciberseguridad Industrial, en el marco de la normativa IEC 62443, con aplicación a Subestaciones Eléctricas. Se realizará un análisis de riesgos, estudiando cada uno de los posibles escenarios, se proponen medidas de mitigación de riesgos. Finalmente se evaluará la mejora del nivel de riesgo, y se comprobará que se encuentra dentro del nivel que se ha establecido como aceptable.

1.1.2 Objetivos específicos

- Estudio de la situación actual de la ciberseguridad en los entornos industriales, concretamente en el sector energético: la normativa referente de ciberseguridad industrial, incidentes pasados, protocolos de comunicación industriales, modelado de amenazas, modelado de ataques y Cyber Kill Chain.

- Creación de un Plan Director de Ciberseguridad para el entorno OT (Operational Technology, en español: Tecnología Operacional). Conocer la situación actual, establecer la estrategia de la organización, definir proyectos e iniciativas, clasificar y priorizar, aprobación del plan, puesta en marcha y análisis del cumplimiento de los requisitos y objetivos del Plan Director de Ciberseguridad.

- Propuesta de aquellas medidas de mitigación de riesgos más prioritarias:
    - Diseño de una arquitectura de red segura.
    - Análisis de los IDS disponibles en el mercado.
    - Análisis de los SIEM disponibles en el mercado.

- Creación de un entorno virtual de simulación, en el cual, se simularán una serie de ciberataques clasificados en la matriz MITRE industrial. Se comprobará que los ataques son detectados por el IDS. De esta manera, se pretende validar el escenario propuesto para el Plan Director de Ciberseguridad.

1.2 Gestión y planificación del trabajo

El tiempo de realización del proyecto es de 375 horas, repartido en 4.7 meses, desglosado en una dedicación de 20 horas semanales.

Figura 1. Diagrama de Gantt de la planificación del proyecto.

1.2.1 Requisitos

El Plan Director de Ciberseguridad Industrial que se lleva a cabo, debe seguir los requisitos de la norma IEC 62443-3-3: "Requisitos de seguridad del sistema y niveles de seguridad" [2], los cuales se clasifican en los siguientes Requisitos Fundamentales (FR – Fundamental Requirements) y en los requisitos individuales del sistema de control (SR), que servirán para evaluar las capacidades que debe cumplir el proyecto.

- **FR 1. Control de identificación y autenticación**
  - SR 1.1. Identificación y autenticación de usuarios humanos
  - SR 1.2. Identificación y autenticación de procesos de software
  - SR 1.3. Gestión de cuentas
  - SR 1.4. Gestión de identificadores
  - SR 1.5. Gestión de autenticadores
  - SR 1.6. Gestión de acceso inalámbrico
  - SR 1.7. Fortaleza de la autenticación basada en contraseña
  - SR 1.8. Certificados de infraestructura de clave pública (PKI)
  - SR 1.9. Fortaleza de la autenticación de clave pública
  - SR 1.10. Retroalimentación del autenticador
  - SR 1.11. Intentos fallidos de inicio de sesión
  - SR 1.12. Aviso de uso del sistema
  - SR 1.13. Acceso a través de redes que no son de no confianza
- **FR 2. Control de uso**
  - SR 2.1. Aplicación de la autorización
  - SR 2.2. Control de uso inalámbrico
  - SR 2.3. Control de uso para dispositivos portátiles y móviles
  - SR 2.4. Código móvil
  - SR 2.5. Bloqueo de la sesión

    - SR 2.6. Terminar una sesión remota
    - SR 2.7. Control de las sesiones simultáneas
    - SR 2.8. Eventos auditables
    - SR 2.9. Capacidad de almacenamiento de datos de auditoría
    - SR 2.10. Respuesta a los fallos de procesamiento de auditorías
    - SR 2.11. Marcas de tiempo
    - SR 2.12. No rechazo
- **FR 3. Integridad del sistema**
    - SR 3.1. Integridad de la comunicación
    - SR 3.2. Protección contra códigos maliciosos
    - SR 3.3. Verificación de la funcionalidad de la seguridad
    - SR 3.4. Integridad del software y de la información
    - SR 3.5. Validación de entrada
    - SR 3.6. Salida determinista
    - SR 3.7. Tratamiento de errores
    - SR 3.8. Integridad de la sesión
    - SR 3.9. Protección contra la información de auditoría
- **FR 4. Confidencialidad de los datos**
    - SR 4.1. Confidencialidad de la información
    - SR 4.2. Persistenia de la información
    - SR 4.3. Uso de criptografía
- **FR 5. Flujo de datos restringido**
    - SR 5.1. Segmentación de red
    - SR 5.2. Protección de los límites de la zona
    - SR 5.3. Restricciones de comunicación entre personas de propósito general
    - SR 5.4. Partición de aplicaciones
- **FR 6. Respuesta oportuna a los Incidentes**
    - SR 6.1. Accesibilidad de los registros de auditoría
    - SR 6.2. Supervisión contínua
- **FR 7. Disponibilidad de recursos**
    - SR 7.1. Protección contra la denegación de servicio
    - SR 7.2. Gestión de recursos
    - SR 7.3. Copia de seguridad del sistema de control
    - SR 7.4. Recuperación y reconstrucción del sistema de control
    - SR 7.5. Alimentación de emergencia
    - SR 7.6. Ajustes de configuración de red y seguridad
    - SR 7.7. Funcionalidad mínima
    - SR 7.8. Inventario de componentes del sistema de control

1.2.2 Hitos

Se establecen los hitos en el desarrollo del proyecto para establecer los puntos de control en la evaluación del trabajo. La fecha de los hitos se encuentra en la Figura 1, al finalizar las tareas asociadas a los mismos.

- **Hito 1.** Planificación del trabajo
- **Hito 2.** Estudio preliminar del estado de la ciberseguridad en los entornos industriales
- **Hito 3.** Plan de Seguridad
- **Hito 4.** Definir la red del entorno industrial
- **Hito 5.** Comparativo de IDS e IPS
- **Hito 6.** Comparativo de SIEMs
- **Hito 7.** Escenario virtual
- **Hito 8.** Pruebas sobre el escenario virtual
- **Hito 9.** Conclusiones

1.3 Normativa referente de ciberseguridad industrial

El estándar que se aplica a nivel internacional para una gestión efectiva de la seguridad de la tecnología de la información (IT) es ISO/IEC 27001/2 [6]. Según la alianza global de ciberseguridad ISA [7], algunas organizaciones han tratado de abordar su infraestructura de tecnología operativa (OT) bajo este mismo sistema de gestión, aprovechando que IT y OT coinciden en muchos puntos. La norma ISA/IEC 62443 [8] trata de estandarizar esta cuestión, manteniendo la conformidad con ISO/IEC 27001 a través de enfoques comunes siempre que sea posible.

El objetivo de IEC 62443 es la seguridad de los sistemas de control y automatización industrial y su alcance se define en el documento "Quick Start Guide: An Overview of ISA/IEC 62443 Standards" [9] como "Un conjunto de personal, hardware, software y políticas que intervienen en el funcionamiento de proceso industrial y que pueden afectar o influir en su funcionamiento seguro, protegido y fiable". El estándar ISA/IEC 62443 se organiza en cuatro grupos principales, como se puede ver en la Figura 2.

1. **General:** Documentos comunes a toda la serie.
    - 62443-1-1: Terminología, conceptos y modelos.
    - 62443-1-2: Glosario general de términos y abreviaturas.
    - 62443-1-3: Medidas de conformidad de la seguridad del sistema.
    - 62443-1-4: Seguridad del ciclo de vida del IACS (Industrial Automation Control System – Sistema de Control y Automatización Industrial) y casos de uso.
2. **Políticas y procedimientos:**
    - 62443-2-1: Establecer un programa de seguridad en IACS.
    - 62443-2-2: Calificación del programa de seguridad de IACS.
    - 62443-2-3: Gestión de parches en el entorno IACS.
    - 62443-2-4: Requisitos del programa de seguridad para proveedores de servicio en IACS.
    - 62443-2-5: Orientación para propietarios de los activos en IACS.
3. **Requisitos del sistema:**
    - 62443-3-1: Tecnologías de seguridad para IACS.
    - 62443-3-2: Evaluación de riesgos de seguridad para diseño de sistemas.
    - 62443-3-3: Requisitos de seguridad de sistemas y niveles de seguridad.
4. **Requisitos de los componentes:**
    - 62443-4-1: Requisitos de seguridad del ciclo de vida de desarrollo de producto.
    - 62443-4-2: Requisitos técnicos de seguridad para componentes del IACS.

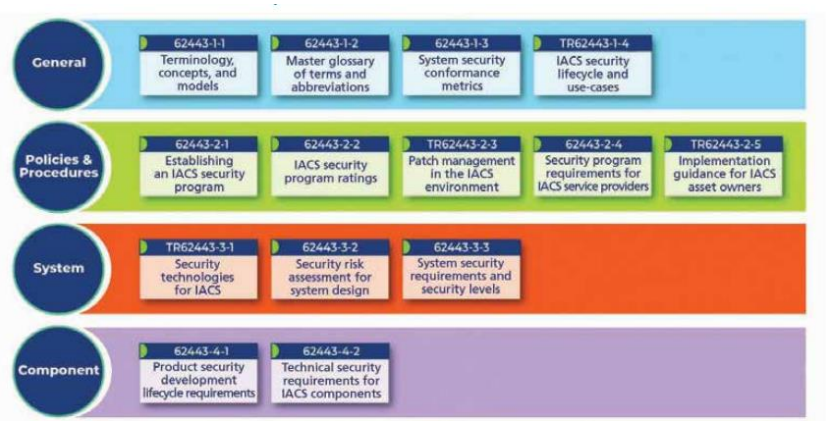

Figura 2. La serie ISA/IEC 62443 [9].

Para el desarrollo de este documento, se han tenido presentes, especialmente "UNE-EN IEC 62443-3-2:2021: Evaluación del riesgo de seguridad para el diseño de sistemas" [8] y "UNE-EN IEC 62443-3-3: Requisitos de seguridad del sistema y niveles de seguridad" [2]. Se expone que existe una normativa de seguridad de la información específica para subestaciones eléctricas: "UNE-EN IEC 62351-3:2023: Gestión de sistemas de potencia e intercambio de información asociada. Seguridad de datos y comunicaciones" [10]. En el apartado "4.1. Normativa" se profundiza más acerca de cómo se aplica esta normativa y de su compatibilidad con el resto.

1.4 Incidentes de ciberseguridad industrial

Un incidente de ciberseguridad se refiere a un evento que puede ser dirigido o accidental que provoca una alerta en los sistemas de detección de seguridad. Tal y como menciona Agustín Valencia, profesor del Centro de Ciberseguridad Industrial [11], se requiere de un personal específico con formación y herramientas para monitorizar eventos de seguridad y detección de intrusiones, para vigilar y proteger una base de activos. A esta organización de personas, se le denomina Centro de Operaciones de Seguridad (SOC – Security Operations Center).

Un SOC enfocado a IACS tiene una serie de complejidades asociadas, ya que el impacto de un ciberataque supone consecuencias severas como:

- Peligro para la seguridad o la salud pública o de los trabajadores.
- Daños al medio ambiente.
- Daños a los equipos controlados.
- Pérdida de la integridad del producto.
- Pérdida de confianza del público o de la reputación de la empresa.
- Violación de requisitos legales o reglamentarios.
- Pérdida de información patentada o confidencial.
- Pérdidas financieras.
- Impacto en la seguridad de la entidad, local, estatal o nacional.

La primera consecuencia mencionada es única de los sistemas ciberfísicos y no está presente típicamente en sistemas IT.

1.4.1 Incidentes en los últimos años

A continuación, se recogen una serie de ciberataques a IACS destacados que han ocurrido en los últimos años.

Tabla 1. Ciberataques destacados a IACS [9].

Date	Target	Method
2000	Australian Sewage Plant	Insider
2010	Iran Uranium Enrichment	Stuxnet
2013	ICS Supply Chain attack	Havex
2014	German Steel Mill	
2015	Ukraine Power Grid	BlackEnergy, KillDisk
2016	Ukraine Substation	CrashOverride
2017	Global shipping company	NotPetya
2017	IoT DDos attack	BrickerBot
2017	Health care, Automotive	WannaCry
2017	Saudi Arabia Petrochemical	TRITON/TRISIS
2019	Norwegian Aluminum Company	LockerGaga

Entre ellos, se va a comentar al caso de Stuxnet, ya que fue un ataque dirigido a una planta energética. En enero de 2010, los inspectores de la Agencia Internacional de Energía Atómica, durante su visita a una planta nuclear en Natanz, Irán, observaron que las centrifugadoras empleadas para el proceso de enriquecimiento de uranio presentaban fallos inesperados. Éste fenómeno se repitió cinco meses después, y entonces fue cuando se detectó que fue causado por un malware. Concretamente, un gusano informático llamado "Stuxnet", que tomó el mando de 1000 máquinas que colaboraban en la producción de materiales nucleares y les dio instrucciones de autodestruirse. Como se menciona en el artículo de 2015 de la BBC [12], se considera la primera vez que un ataque cibernético consigue dañar infraestructura física. Se cree que el gusano logró penetrar en el sistema debido a que alguien insertó físicamente una memoria USB en un ordenador que pertenecía a la red de la planta.

Se va a analizar el caso anteriormente mencionado, de la misma manera que se hará en los distintos Escenarios de Riesgos para la evaluación del Plan de Ciberseguridad:

Tabla 2. Ejemplo de análisis del escenario de riesgo en el caso de Stuxnet.

Activos	**Agentes**
• Lógica en ejecución en controladores y/o PC SCADA • Equipos, máquinas y/o instalaciones	• Personal propio y de terceras partes • Estados
Factores de riesgo	
A. Uso de dispositivos USB para el intercambio de información relevante para el proceso productivo B. Segmentación inadecuada de la red corporativa con la red ICS. C. Segmentación inadecuada en el acceso de terceros para el mantenimiento de sistemas. D. Segmentación inadecuada entre los niveles de control y supervisión en la red de control.	
Contexto	
Un agente externo a la organización accedió a la planta industrial, introdujo un dispositivo USB a un ordenador de la red e infectó al dispositivo. Debido a la pobre securización de la red, el gusano logró extenderse al resto de la planta.	

1.4.2 Actores de amenazas

Los actores de amenazas son grupos o individuos malintencionados que pretenden explotar las debilidades de un sistema de información para afectar a los datos, sistemas o redes de las víctimas. Se pueden clasificar en los siguientes 6 grupos [13]: Cibercriminales, Hacktivistas, Estados, Ciberterroristas, "Script kiddies" e "Insiders".

1. **Cibercriminales**: Atacan a las organizaciones a través de la extorsión o la divulgación de datos comprometidos para obtener beneficios económicos o personales. Son capaces de llevar a cabo campañas complejas y sofisticadas utilizando herramientas y servicios cibernéticos disponibles en los mercados ilegales en línea. En muchos casos incluso ofrecen su servicio a terceros a cambio de una compensación económica. Existen numerosos grupos de cibercriminales conocidos que han comprometido Sistemas de Control Industrial, tal y como se describe en la Tabla 3.

Tabla 3. Algunos cibercriminales conocidos en Sistemas de Control Industrial.

Actor de amenazas	Descripción	Sector principal	Motivación
HEXANE [14]	Se encontró por primera vez en 2017. Se observó que este grupo tenía como objetivo empresas petroleras y de gas de Oriente Próximo. Además, y a diferencia de otros grupos, también se dirigía a proveedores de telecomunicaciones en Oriente Próximo, Asia Central y África.	Energía, Gas y petróleo, Telecomunicaciones	Robo de información y espionaje
Lockbit [15]	LockBit, que se unió al negocio del ransomware como servicio (RaaS) en septiembre de 2019, está impulsado por procesos automatizados para propagarse rápidamente a través de la red de la víctima, identificar sistemas valiosos y bloquearlo, dejando pocos rastros.	Aviación, Defensa, Energía, Financiero, Salud, Transporte	Beneficios económicos
Magnallium [16]	También conocido como APT33, es un grupo capaz que ha llevado a cabo operaciones de ciberespionaje desde al menos 2013. Se piensa que APT33 trabaja a las órdenes del gobierno iraní.	Aviación, Defensa, Educación. Energía, Financiero, Gobiernos, Salud, Tecnología, Manufactora, Comunicación, Gas y petróleo	Robo de información, Sabotaje y destrucción

2. **Hacktivistas**: Individuo o grupo de personas que comprometen sistemas con fines políticos o sociales. Las acciones pretenden causar un daño significativo a la reputación de sus objetivos.

Tabla 4. Algunos hacktivistas conocidos en Sistemas de Control Industrial.

Actor de amenazas	Descripción	Sector principal	Motivación
Lapsus$ [17]	Su primer ataque fue el 10 de diciembre de 2021, contra el Ministerio de Salud de Brasil, comprometiendo los datos de las vacunas de COVID-19 del país. Se centra en monetizar sus operaciones exclusivamente a través de filtraciones de datos anunciadas en Telegram sin el uso de ransomware.	Salud, Telecomunicaciones, Tecnología	Beneficios económicos
Killnet [18]	Lanzada a finales de febrero de 2022. Más de 89.000 suscriptores en su canal de Telegram, organizados en una estructura de tipo militar con una clara jerarquía descendente. Consta de múltiples escuadrones especializados para realizar ataques, todos responden al mando principal.	Salud	Robo de información y espionaje

3. **Estados**: patrocinan grupos de amenazas que lanzan ataques contra gobiernos y organizaciones extranjeras para promover sus objetivos geopolíticos. Con frecuencia son los actores de amenazas más sofisticados, con recursos y personal dedicados, y una amplia planificación y coordinación.

Tabla 5. Algunos ciberataques conocidos realizados por Estados en Sistemas de Control Industrial (1).

Actor de amenazas	Descripción	Sector principal	Motivación
Operation Olympic Games [19]	El expresidente de EEUU, Barack Obama ordenó en secreto ataques cada vez más sofisticados contra los sistemas informáticos que gestionan las principales instalaciones de enriquecimiento nuclear de Irán, ampliando significativamente el primer uso sostenido de ciberarmas por parte de EEUU. [20] Los expertos en seguridad informática que empezaron a estudiar el gusano, desarrollado por Estados Unidos e Israel, le dieron un nombre: Stuxnet.	Energía	Robo de información y espionaje, Sabotaje y destrucción

Tabla 6. Algunos ciberataques conocidos realizados por Estados en Sistemas de Control Industrial (2).

Actor de amenazas	Descripción	Sector principal	Motivación
Silent Chollima [21]	Se cree que está dirigido por el Gobierno norcoreano, motivado principalmente por el beneficio económico como método para eludir las sanciones impuestas desde hace tiempo contra el régimen. Los medios de comunicación se hicieron eco de ellos por primera vez en 2013 con una serie de ataques coordinados contra varias emisoras e instituciones financieras surcoreanas utilizando DarkSeoul, un programa de limpieza que sobrescribe secciones del registro de arranque maestro de las víctimas.	Aerospacial, Defensa, Energía, Ingeniería, Financiero, Gobiernos, Salud, Comunicación, Transporte y logística, Tecnología, Intercambios de Bitcoin	Robo de información y espionaje, Sabotaje y destrucción, Beneficios económicos
Wicked Panda [22]	Surgió en China como una banda de ciberdelincuentes tradicionales, cuyas habilidades técnicas se empleaban para perpetrar fraudes financieros. Basándose en el uso de nombres de dominio que registraron, el grupo comenzó en el negocio de productos antivirus falsos/robados en 2007. En 2009, el grupo se dedicó a atacar a empresas de juegos de Corea del Sur mediante un programa malicioso de robo de datos y archivos.	Videojuegos, Aviación, Defensa, Educación, Financiero, Gobiernos, Salud, Farmacéutico, Tecnología, Telecomunicaciones	Robo de información y espionaje

4. **Ciberterroristas**: Los ciberterroristas atacan sistemas para interrumpir o destruir servicios e infraestructuras críticos de una nación, sector u organización concretos. Se diferencian de los ciberdelincuentes por su motivación: los delincuentes están motivados por la recompensa, mientras que los terroristas actúan por los posibles efectos.

Tabla 7. Algunos grupos ciberterroristas en Sistemas de Control Industrial.

Actor de amenazas	Descripción	Sector principal	Motivación
NoName057(16)	Grupo hacktivista ciberterrorista pro-ruso creado en marzo de 2022 centrado principalmente en la interrupción de sitios web importantes para las naciones críticas con la invasión rusa de Ucrania.	Comunicación, Transporte, Energía	Robo de información y espionaje, Beneficios económicos

5. **“Script Kiddies”**: Personas que descargan una herramienta sin saber necesariamente ni preocuparse por su funcionamiento. Utiliza técnicas, programas y scripts existentes y bien conocidos para encontrar y explotar las debilidades de los ordenadores conectados a Internet. Sus ataques son aleatorios y con poca comprensión de las herramientas que utilizan, cómo funcionan y el daño que causan. Motivados por razones personales o simples como buscar atención, divertirse, crear el caos o venganza. Existen foros en internet especializados en actividades fraudulentas, los más activos en la Deep web son: XSS, Exploit, Breached Forums o Helium Forum.

6. **“Insiders”**: Personas estrechamente vinculadas a una organización y que goza de acceso autorizado abusa de sus privilegios de acceso para afectar negativamente a la información o sistemas claves de la empresa. Esta persona no tiene por qué ser un empleado. Los proveedores externos, contratistas y socios también podrían ser amenazas. Estadísticas del año 2016 de amenazas realizadas por insiders revelan que el 69% de los encuestados afirmaron que sus organizaciones habían sufrido intentos (fallidos o exitosos) o corrupción de sus datos en los últimos 12 meses [23].

Para determinar quien ha realizado un ciberataque, se requiere de un análisis profundo del mismo. En algunos casos, puede que sean distintos tipos de actores trabajando colaborativamente, como, por ejemplo, cibercriminales trabajando para gobiernos. En muchos casos, los grupos se denominan así mismos con distintos nombres y actúan desde distintas ubicaciones geográficas, haciendo aún más compleja esta tarea.

2 CIBERSEGURIDAD EN ENTORNOS INDUSTRIALES

Para proveer a las empresas industriales la seguridad necesaria en sus redes, con el fin de prevenir y detectar posibles incidencias, es necesario realizar un inventario de activos, un diagnóstico de ciberseguridad, diseñar/ejecutar un Plan Director de Ciberseguridad y aplicar normativa y estándares [24]. En este apartado se detallan los elementos de los Sistemas de Control y Automatización Industrial, qué protocolos de comunicación se usan en los entornos industriales, para poder enfocarnos en ellos a la hora de detectar intrusiones y se comentará como se modelan las amenazas y ataques específicamente en redes OT.

2.1 Sistemas de Control y Automatización Industrial

Los sistemas de control y automatización industrial (IACS - Industrial Automation and Control System) abarcan distintos tipos de sistemas de control entre los que se encuentran [25]:

- **Controladores Lógicos Programables (PLC):** Autómata programable, utilizados como dispositivos de campo, son más económicos y flexibles que las RTU.
- **Unidades Terminales Remotas (RTU):** Microprocesadores que obtienen señales de sensores para procesarlas remotamente.
- **Sistemas de Control Distribuido (DCS**): Las funciones de adquisición y control son realizadas por un conjunto de microprocesadores distribuidos cerca de los dispositivos controlados o de los instrumentos monitorizados.
- **Sistemas de Supervisión Control y Adquisición de Datos (SCADA):** Conjunto de RTUs que colectan datos de campo a una estación principal. Dicha estación principal permite mostrar los datos adquiridos y realizar tareas de control remoto. Los datos se toman en tiempo real, lo que permite optimizar la operación de la planta. Otra ventaja es que las operaciones son más eficaces, fiables y, lo que es más importante, más seguras. Todo ello se traduce en un menor coste de explotación en comparación con los anteriores sistemas no automatizados.

Para el desarrollo de este proyecto, nos centraremos en los sistemas SCADA, que tienen los siguientes componentes:

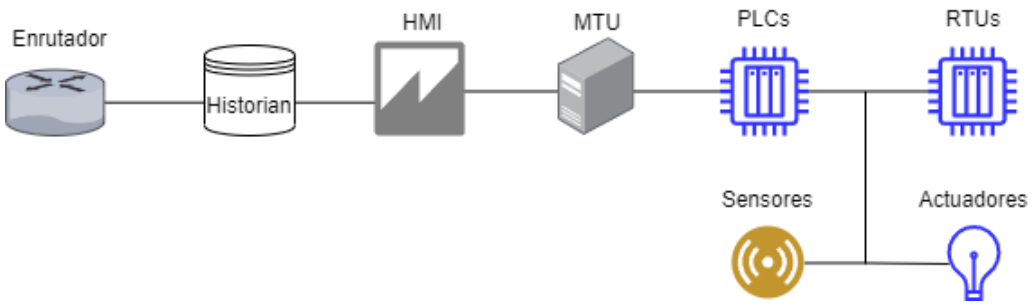

Figura 3. Componentes de un sistema SCADA.

Los componentes de la Figura 3, se describen a continuación:

- **HMI**: Interfaz hombre-máquina. Permite al operador monitorizar los datos y controlar acciones mediante una pantalla táctil.
- **Sistema de supervisión (MTU)**: Se trata de un ordenador que recopila los datos del proceso mediante RTUs y permite enviar comandos.
- **Unidades Terminales Remotas (RTU):** Descrito en la página anterior.
- **Controladores Lógicos Programables (PLC):** Descrito en la página anterior.
- **Historian:** Se trata de una base de datos, encargada de almacenar datos temporalmente para poder ser consultados.
- **Red de comunicación**: Dispositivos de red (switches, routers, firewall…) que permiten la comunicación entre los elementos del sistema.
- **Sensores**: Dispositivos que detectan magnitudes físicas o químicas, que se denominan variables de instrumentación, y las convierten en señales.
- **Actuadores**: Dispositivos mecánicos que provocan un movimiento sobre otro dispositivo mecánico.

2.2 Protocolos de comunicación industriales

Los sistemas de control industriales utilizan protocolos de comunicación específicos para mayor fiabilidad y eficiencia. Están acompañados de estándares para que los dispositivos interactúen eficazmente entre sí.

La industria ha pasado de utilizar sistemas electromecánicos con comunicaciones del tipo M2M (Machine to Machine – Máquina a Máquina) mediante protocolos serie, a comunicaciones tipo cliente-servidor con protocolos sobre Ethernet y TCP/IP. Esto se debe en gran medida a que facilita la integración con la infraestructura IT (Information Technology – Tecnologías de la Información), y, por otra parte, se debe al auge del Internet de las Cosas (IoT - Internet of Things) que también utiliza la misma pila de protocolos. Lo cual, permite mayor eficiencia, menores costes de integración y mejor rendimiento, pero hace que los sistemas sean más vulnerables a ciberataques internos y externos de la red.

En 2019, HMS Networks, empresa internacional dedicada a la comunicación industrial, publicó un artículo [26], en el cual, mostraba el crecimiento anual de protocolos industriales de tres ámbitos diferentes: buses de campo, comunicaciones inalámbricas y ethernet industrial.

En la Figura 4, se aprecia como el uso de protocolos de buses de campo disminuye por primera vez en la historia, obteniendo un -5% de crecimiento frente al 6% del año anterior. A su vez, las comunicaciones inalámbricas siguen siendo las menos utilizadas, debido a que puede haber desconexiones por baja cobertura, ruido electromagnético, interferencias, entre otros problemas y la prioridad de los sistemas de control es la robustez y la respuesta en tiempo real. El protocolo Ethernet Industrial sigue siendo el ganador en el sector de la automatización, a causa de la necesidad de un alto rendimiento y la integración con sistemas IT y/o aplicaciones IoT industrial.

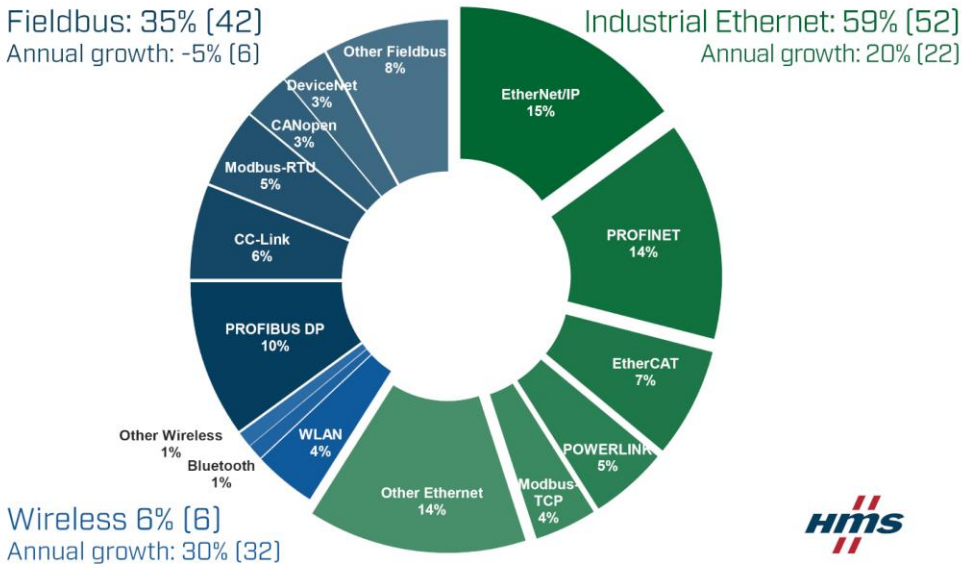

Figura 4. Cuotas de mercado de redes industriales en 2019 según HMS [26].

Se ha recopilado de los protocolos más usados la siguiente información, de diversas fuentes como "Protocols and Network Security in ICS Infrastructures, de INCIBE" [27] y en las páginas correspondientes a las organizaciones encargadas de estandarizar cada uno de los protocolos.

En la Tabla 8, se recoge el estándar, organización, tipo de protocolo (abierto o comercial), configuraciones que admite, capas del modelo OSI que implementa, de los protocolos: EtherNet/IP, Profinet, EtherCAT, Powerlink, Modbus TCP, IEC 60870-5-104, DNP3, BACnet, CIP, ControlNet, Profibus, OCP, S7 y MQTT.

La mayoría de los protocolos son abiertos, y disponen de pilas de protocolo listas para integrar en los dispositivos, desarrolladas por las propias organizaciones o por personas independientes. Pero es cierto que también hay muchas implementaciones comerciales, de estos mismos protocolos, ya que ofrecen otra serie de servicios y utilidades adicionales como el mantenimiento, simuladores, analizadores y depuradores del protocolo. Esto permite realizar pruebas en escenarios reales o virtuales para comprobar su seguridad. Además, muchos de ellos también disponen de simuladores gratuitos, por lo que no se necesitaría implementar la pila en un dispositivo.

Se observa como la mayor parte de los protocolos, en su versión básica, no ofrecen protecciones de seguridad como la autenticación o el cifrado de los datos. Algunos de ellos tienen implementaciones mejoradas que sí lo ofrecen, o incluso se pueden llegar a integrar el cifrado y la autenticación usando SSL (protocolo de seguridad en internet basado en el cifrado [28]).

Además, los protocolos más usados (según la Figura 4), tienen en común que implementan hasta la capa de transporte en el modelo OSI. Cabe destacar, que los protocolos industriales más utilizados son del ámbito de la automatización y control, pero también encontramos protocolos como BACnet (Building Automation and Control Networks), cuya aplicación es la comunicación entre distintos dispositivos dentro de un edificio (alarmas, sensores de paso, climatización…).

Tabla 8. Características de los protocolos industriales.

Protocolo	Estándar	Organización	Abierto/Comercial	Configuraciones	Capa MAC	Capa IP	Capa Transporte	Capa Aplicación	Autenticación	Cifrado
EtherNet/IP	ODVA association	Rockwell Automation	Abierto	publicador/suscriptor (mensajes implícitos) cliente/servidor (mensajes explícitos)	Si	Si	Si	No	No	No
Profinet	PROFIBUS & PROFINET International (PI)	Siemens	Abierto	publicador/suscriptor cliente/servidor	Si	Si	Si	No	No	No
EtherCAT	ETG	Beckhoff	Comercial	maestro/esclavo	Si	Si	Si	No	No	No
POWERLINK (EPL)	EPSG	Bernecker & Rainer	Abierto	maestro/esclavo	Si	Si	Si	No	No	No
Modbus TCP	Modbus Organization	Schneider Electric	Abierto	cliente/servidor (TCP) maestro/esclavo (RTU)	Si	Si	Si	No	No	No
IEC 60870-5-104	IEC 60870-5-104	IEC TC 57 (WG 03)	Abierto	cliente/servidor	Si	Si	Si	Si	No	No
DNP3	IEEE 1815-2012	DNP Users Group	Abierto	cliente/servidor	Si	No	No	No	Si (DNP3 Secure)	No
BACnet	ANSI 135-2016	BACnet committee	Abierto	cliente/servidor	No	Si	No	Si	Si	Si
CIP	ODVA association	Rockwell Automation	Abierto	publicador/suscriptor (mensajes implícitos) cliente/servidor (mensajes explícitos)	Si	Si	Si	Si	No	No
ControlNet	ODVA association	Rockwell Automation	Abierto	maestro/esclavo	No	No	No	No	No	No
Profibus	PROFIBUS & PROFINET International (PI) DIN19245 EN50170	Siemens	Abierto	maestro/esclavo	No	No	Si	No	No	No
OPC	IEC 62541-1:2020	Microsoft	Abierto	cliente/servidor	Si	Si	Si	No	Si (OPC UA)	No
S7	Basado en RFC1006	Siemens	Comercial	cliente/servidor	No	No	Si	Si	No	No
MQTT	ISO/IEC 20922	OASIS	Abierto	publicador/suscriptor	Si	Si	Si	Si	No	No

2.3 Nomenclatura de ciberseguridad en entornos industriales

A continuación, se detalla el modelado de amenazas y de ataques empleados en los Sistemas de Control Industrial. Concluyendo con la Cyber Kill Chain, que explica las distintas fases de un ciberataque.

2.3.1 Modelado de amenazas en Sistemas de Control Industrial

Una amenaza en ciberseguridad es cualquier peligro potencial o evento dañino que pueda explotar una vulnerabilidad y causar daño a un sistema, organización o individuo [1].

El modelo de referencia para guiar las políticas de seguridad de la información en sistemas IT es el modelo CIA (Confidential, Integrity and Availability – Confidencialidad, Integridad y Disponibilidad). Se basa en mantener la Confidencialidad, integridad y disponibilidad de los sistemas. Hay expertos que no están de acuerdo en aplicar este modelo en los entornos industriales de la actualidad, debido a que no se ajustan a las nuevas necesidades generadas por la era de los sistemas embebidos (IoT y OT) y por las capacidades emergentes de la inteligencia artificial.

Existen varias aproximaciones como "SRP Triad -Best for ICS Cyber Security" [29] o "The CIA Triad Is Insufficient In The Age of AI/OT/IoT" [30]. Ésta última está referenciada en la norma ISA/IEC 62443. Este modelo, representa un mayor espectro de amenazas y simplemente añade el parámetro de seguridad al modelo "CIA" Triad, convirtiéndolo en el nuevo modelo "CIAS". La componente de "seguridad" trata de reducir el riesgo asociado a las tecnologías que podrían fallar o ser manipuladas por actores maliciosos para causar muertes, heridos, enfermedades, daños o pérdida de equipamiento, también asociado con guerra cibernética o terrorismo.

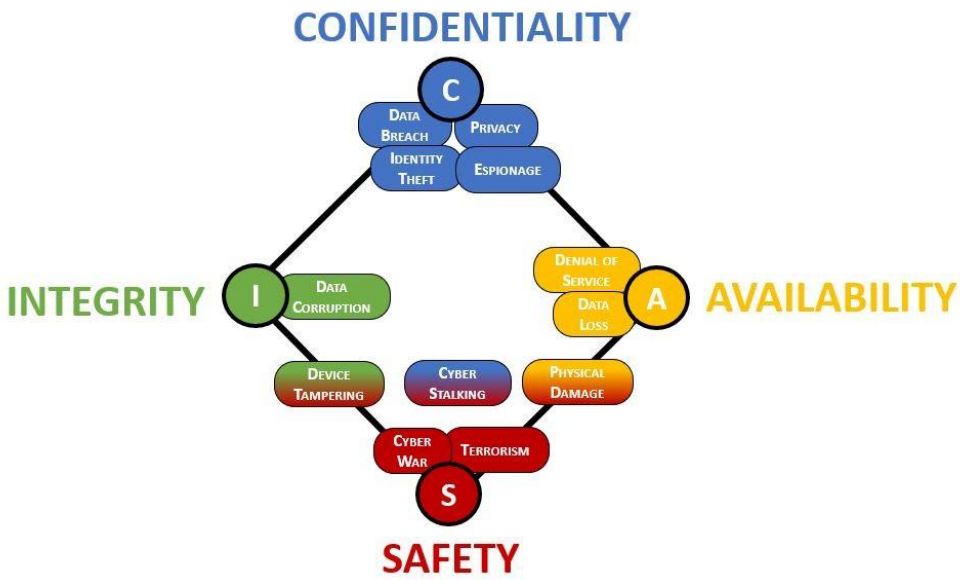

Figura 5. Modelo CIAS [30].

2.3.2 Modelado de ataques en Sistemas de Control Industrial

Un ciberataque es cualquier tipo de actividad maliciosa que intente recopilar, interrumpir, denegar, degradar o destruir recursos del sistema de información o la propia información [31].

Los posibles ataques en una infraestructura industrial evidentemente no son sólo cibernéticos, pueden ser también físicos, como recoge "Attacking IEC-60870-5-104 SCADA Systems" [32], en el que crea un modelo de amenazas clasificando los ataques en estos dos grupos, ataques físicos y ciberataques. Dentro de estos dos grupos se subclasifican en ataques en la alimentación, en el control de datos y en el control de comandos.

Aunque no es el objeto de este trabajo, para prevenir y mitigar los ataques físicos se tendría que definir un Plan Director de Seguridad Física, donde se definirá una infraestructura de CCTV (Circuito Cerrado de Televisión, es decir, sistema de videovigilancia) y CCAA (Controles de Accesos), junto con el personal correspondiente de vigilantes y operadores de seguridad.

Un enfoque adecuado para clasificar los ataques de red en Sistemas de Control Industrial (ICS – Industrial Control Systems), es seguir la matriz de "MITRE ATT&CK para ICS" [33]. Dicha matriz fue creada por MITRE con el propósito de monitorear, recopilar y analizar las amenazas de ciberseguridad, especialmente en entornos industriales. MITRE es una corporación sin ánimo de lucro comprometida con el interés público, que gestiona centros de I+D financiados con fondos federales en nombre de patrocinadores de la Administración estadounidense.

La matriz MITRE para Sistemas de Control Industrial, representada en la Figura 6, constituye una valiosa fuente de datos que permite a los equipos de investigación fortalecer las defensas de los Sistemas de Control Industrial. Se divide en las siguientes categorías: Acceso inicial, Ejecución, Persistencia, Escalada de privilegios, Evasión, Descubrimiento, Movimiento lateral, Recopilación, Comando y control, Función de inhibición de respuesta, Deteriorar el control del proceso e Impacto. Adicionalmente, permite clasificar las tácticas de ataques en un mismo lenguaje común, para que distintos equipos en la comunidad de ciberseguridad identifiquen los ataques adecuadamente.

Una vez se realice el escenario con los componentes correspondientes a la red OT, se harán una serie de ataques que se clasificarán siguiendo esta matriz.

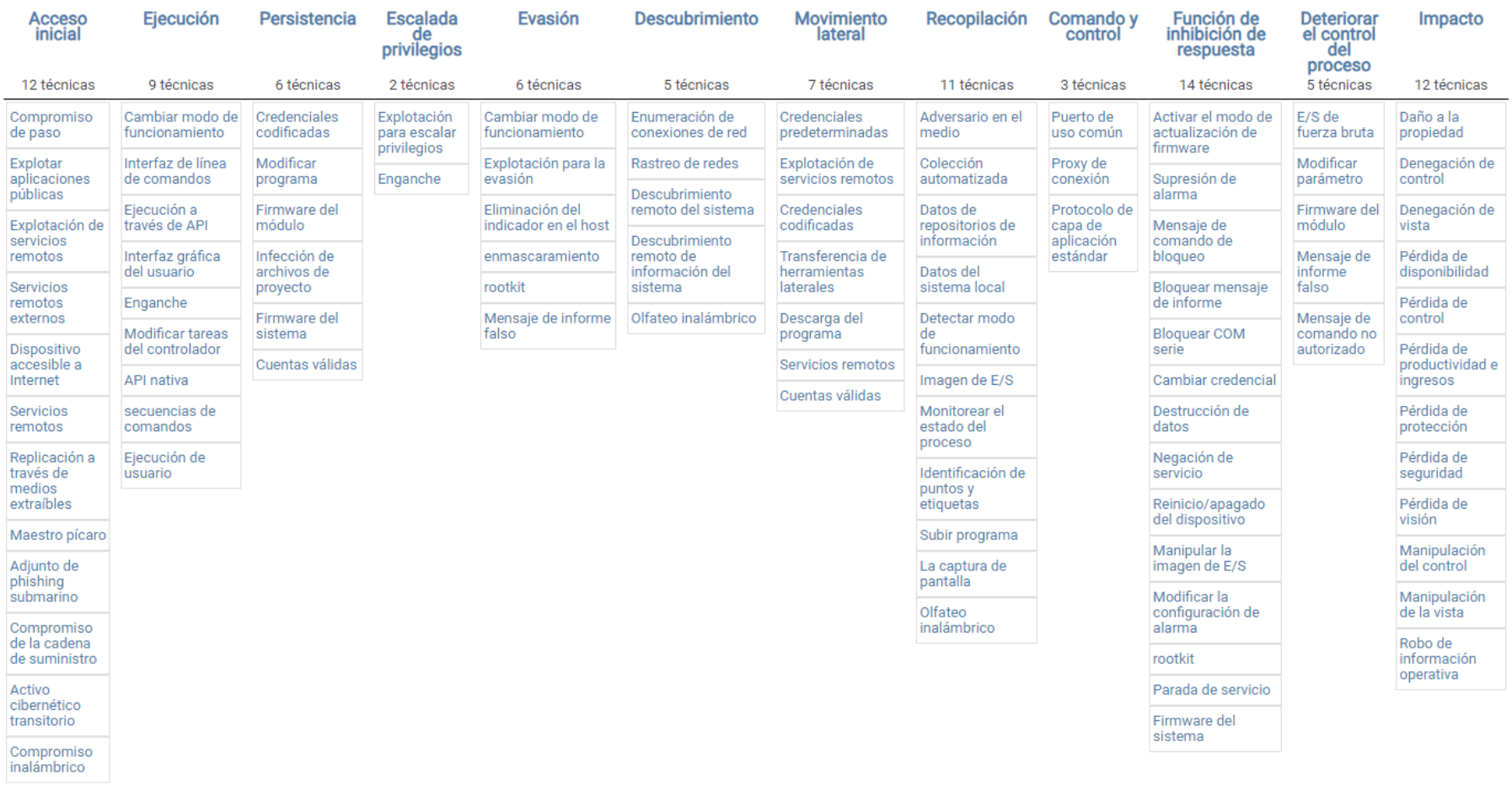

Figura 6. Matriz MITRE para Sistemas de Control Industrial [33].

Además, a través de la herramienta accesible via web [33], se puede acceder a información específica de cada una de las tácticas, como se recoge en los siguientes puntos. Las tácticas son métodos utilizados para alcanzar un objetivo específico, y las técnicas, definen la forma de realizar acciones o estrategias concretas para alcanzar diferentes objetivos definidos dentro de cada táctica [34].

- **Ejemplos de procedimientos:** Ejemplos de procedimientos en los que se han usado esta táctica.

Procedure Examples

ID	Name	Description
S1045	INCONTROLLER	INCONTROLLER can use the CODESYS protocol to download programs to Schneider PLCs.[1][2] INCONTROLLER can modified program logic on Omron PLCs using either the program download or backup transfer functions available through the HTTP server.[1]
S1006	PLC-Blaster	PLC-Blaster utilizes the PLC communication and management API to load executable Program Organization Units. [3]
S0603	Stuxnet	Stuxnet's infection sequence consists of code blocks and data blocks that will be downloaded to the PLC to alter its behavior. [4]
S1009	Triton	Triton leveraged the TriStation protocol to download programs onto Triconex Safety Instrumented System. [5]

Figura 7. Ejemplos de procedimientos en los que se han usado una táctica de la matriz de MITRE.

- **Objetivos**: Activos que son potenciales objetivos de esta táctica.

Targeted Assets

ID	Asset
A0003	Programmable Logic Controller (PLC)
A0010	Safety Controller

Figura 8. Ejemplo de activos objetivo de una táctica de la matriz de MITRE.

- **Mitigaciones**: Medidas que se pueden aplicar para mitigar el impacto de la táctica en cuestión. Será muy útil a la hora de hacer el análisis de riesgos del Plan de Seguridad.

Mitigations

ID	Mitigation	Description
M0801	Access Management	Authenticate all access to field controllers before authorizing access to, or modification of, a device's state, logic, or programs. Centralized authentication techniques can help manage the large number of field controller accounts needed across the ICS.
M0947	Audit	Provide the ability to verify the integrity of programs downloaded on a controller. While techniques like CRCs and checksums are commonly used, they are not cryptographically secure and can be vulnerable to collisions. Preferably cryptographic hash functions (e.g., SHA-2, SHA-3) should be used. [6]
M0800	Authorization Enforcement	All field controllers should restrict the download of programs, including online edits and program appends, to only certain users (e.g., engineers, field technician), preferably through implementing a role-based access mechanism.

Figura 9. Ejemplo de mitigaciones de una táctica de la matriz de MITRE.

- **Detección**: Estrategias a seguir para detectar esta táctica.

Detection

ID	Data Source	Data Component	Detects
DS0015	Application Log	Application Log Content	Monitor devices configuration logs which may contain alerts that indicate whether a program download has occurred. Devices may maintain application logs that indicate whether a full program download, online edit, or program append function has occurred.
DS0039	Asset	Asset Inventory	Consult asset management systems to understand expected program versions.
DS0029	Network Traffic	Network Traffic Content	Monitor for protocol functions related to program download or modification. Program downloads may be observable in ICS automation protocols and remote management protocols.
DS0040	Operational Databases	Device Alarm	Monitor device alarms for program downloads, although not all devices produce such alarms.

Figura 10. Estrategias de detección de una táctica de la matriz de MITRE.

2.3.3 Cyber Kill Chain para Sistemas de Control Industrial

El modelo de Cyber Kill Chain es una conceptualización que se originó en el ámbito militar [35]. Este modelo descompone un ataque en distintas fases, cada una de las cuales es necesaria para lograr su objetivo. Aunque su origen está en el mundo militar, el modelo también se ha adoptado en el campo de la ciberseguridad.

Existen variantes de la Cyber Kill Chain tanto para entornos de Tecnologías de la Información (IT - Information Technology), como para entornos de Tecnología Operativa (OT - Operational Technology). En la Figura 11, se puede apreciar cómo Cyber Kill Chain de IT suele ser la primera fase de un ataque modelado bajo la Cyber Kill Chain de OT.

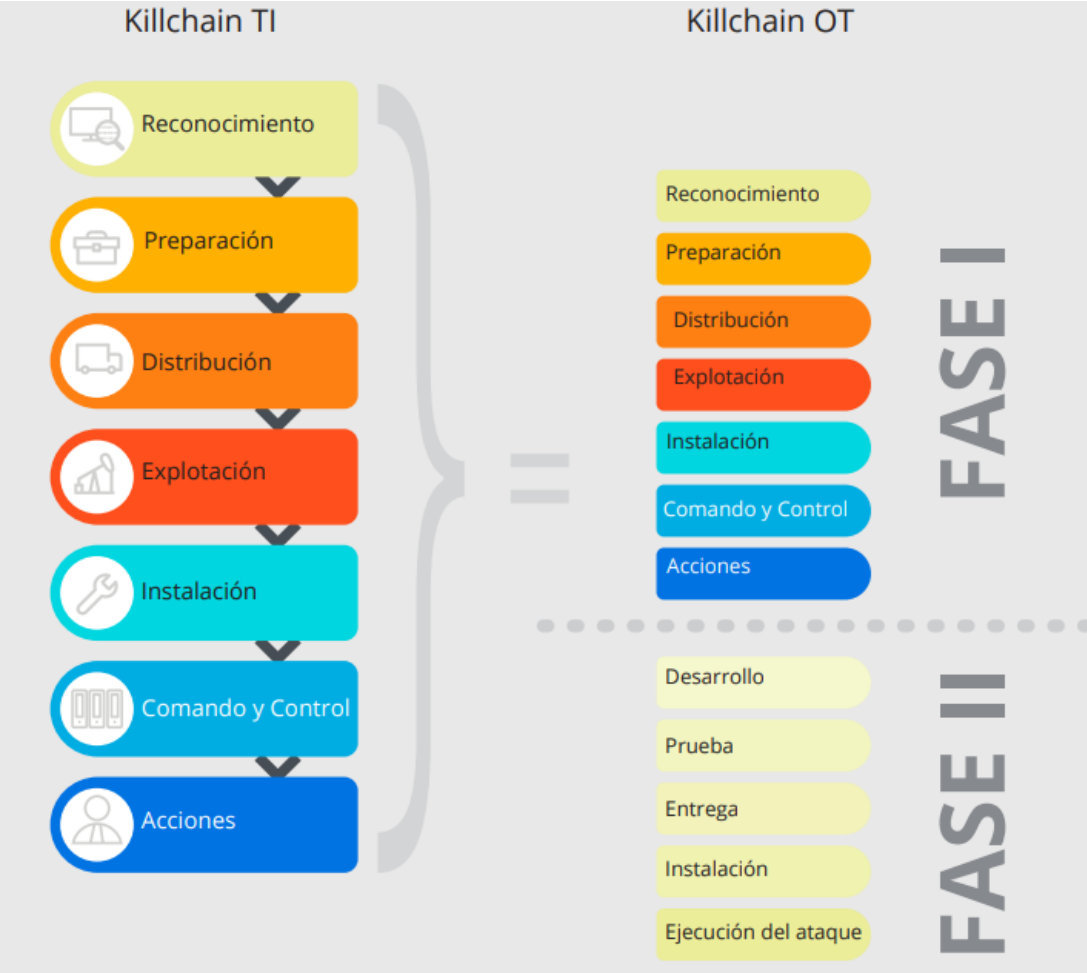

Figura 11. Cyber Kill Chain IT vs OT [35].

Se puede observar como todas estas etapas están contempladas en la matriz MITRE. Lo ideal sería la detección temprana del ataque y no cuando ya haya causado algún impacto.

Fase 1

- **Reconocimiento**: Actividad para obtener información respecto un sistema mediante observación u otros métodos de detección. Puede incluir recabar información del objetivo mediante investigación de fuentes abiertas (OSINT), mediante herramientas como Google o Shodan, que permiten buscar información pública disponible en la web o en redes sociales.

En Sistemas de Control Industrial, la información que interesará al atacante puede incluir información sobre los trabajadores de una planta industrial, la red de comunicaciones de la planta, programas utilizados dentro de la red industrial, versión de los sistemas operativos, cuentas de usuario, información de protocolos de comunicación, políticas, procesos y procedimientos. Con dicha información, se podría investigar acerca de las vulnerabilidades que se pueden explotar del sistema, además de saber qué tráfico es el esperado en la red para poder ocultar la actividad maliciosa.

Por ejemplo, se puede haber detectado qué servidor de VPN utiliza la víctima, qué versión utilizan y estudiar las vulnerabilidades que tiene la misma.

- **Preparación**: Esta etapa puede incluir las subetapas de "militarización" y "selección de objetivos".

    - **Militarización**: Consiste en modificar un archivo aparentemente inofensivo como puede ser un documento de Word o PDF, con el fin de que el adversario intente acceder al sistema.
    - **Selección de objetivos**: El adversario con ayuda de herramientas, identifican víctimas potenciales para explotarlas. Esto conlleva a analizar y prorizar objetivos y la combinación de acciones letales o no letales apropiadas a esos objetivos, en función de la relación entre el esfuerzo requerido durante cierto tiempo, la probabilidad de éxito técnico y el riesgo de detección.

- **Distribución**: El atacante usa un método para interaccionar con la red del entorno industrial, por ejemplo, mediante phishing (envío de un correo electrónico con una URL maliciosa), un archivo PDF modificado o detectando una vulnerabilidad en la VPN del objetivo.

- **Explotación**: El adversario usa una vulnerabilidad para explotarla y poder realizar acciones maliciosas. Por ejemplo, conseguir las credenciales de la VPN de la víctima.

- **Instalación**: Cuando la explotación ha resultado con éxito, el actor malicioso instala una capacidad, como puede ser, acceso remoto, mediante un troyano.

- **Comando y control**: El atacante se conecta a la capacidad previamente instalada.

- **Acciones**: Depende de los objetivos que tenga el atacante, efectuará unas acciones u otras, por ejemplo:

    - Descubrimiento de nueva información o sistemas.
    - Movimiento lateral por la red.
    - Persistencia, es decir, instalar otras puertas de entrada que no puedan ser eliminadas fácilmente.
    - Instalación y ejecución de nuevas capacidades.
    - Capturar las comunicaciones existentes, podiendo así adquirir información crítica, como contraseñas.
    - Obtener datos deseados para exfiltrarlos o cifrarlos y pedir un rescate.
    - Técnicas anti-forenses para evitar ser detectados, como, por ejemplo, borrar logs.

Fase 2

Durante esta fase, el atacante usará el conocimiento adquirido durante la etapa anterior para desarrollar y probar una capacidad que pueda atacar significativamente el ICS. Es posible que la primera fase haya provocado un ataque de por sí afectando a las comunicaciones del sistema.

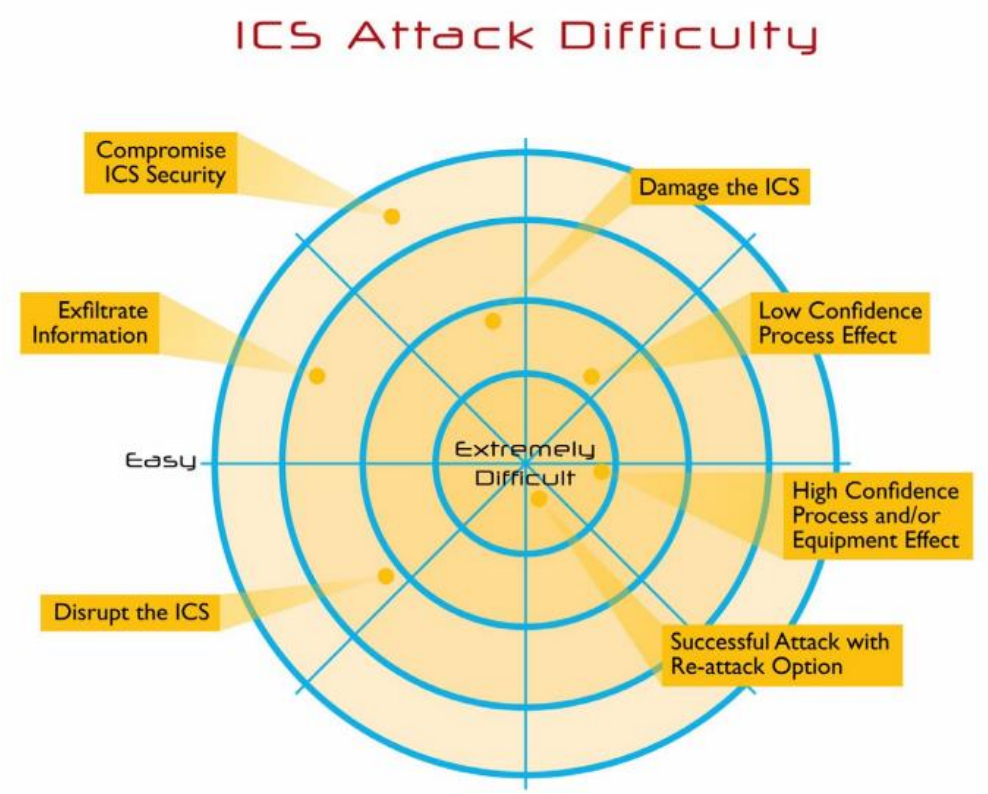

Figura 12. Dificultad de los ciberataques industriales [36].

La complejidad de lanzar un ataque viene determinada por la seguridad de los sistemas, el proceso de monitorizacón y control, la seguridad del diseño y la intencionalidad del impacto.

La Figura 12, desarrollada por el ICSCSI (Instituto de Ciber Seguridad en Sistemas de Control Industrial) [36], representa la dificultad de efectuar distintos tipos de ataques en Sistemas de Control Industrial. Se destaca como los ataques de exfiltración de información y compromiso de la seguridad del ICS, son los considerados más sencillos, mientras que los ataques de afectación a procesos y/o equipos de alta confianza son los más complicados en conjunto con ataques exitosos que pueden volver a repetirse.

3 PLAN DIRECTOR DE CIBERSEGURIDAD

El Plan Director de Seguridad (PDS) varía en función de factores [37] como el tamaño de la empresa, la madurez que tenga la tecnología, el sector de la empresa, la situación legal que regula a la empresa, el ámbito de la información que se maneja, el alcance del proyecto u otros aspectos organizativos. En general, para la elaborar un Plan Director de Seguridad se siguen las siguientes etapas:

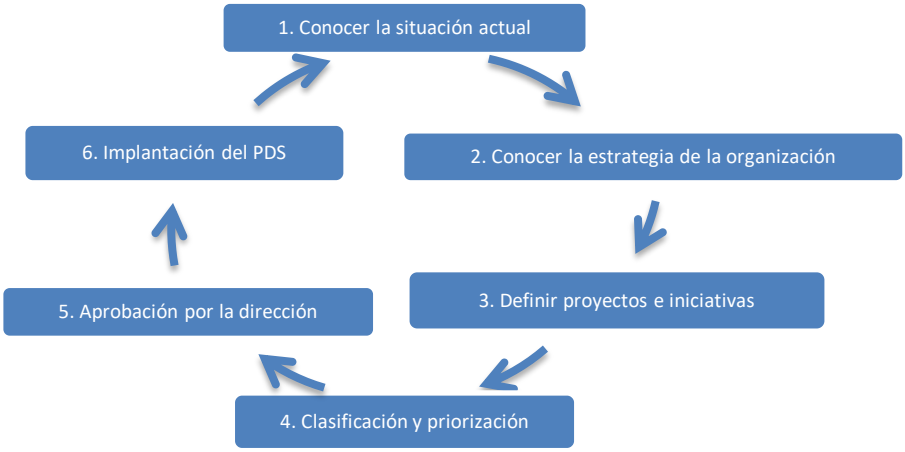

Figura 13. Implantando un Plan Director de Seguridad [37].

Un Plan Director de Seguridad sigue la estrategia de mejora continua, por lo tanto, cuando se finaliza la sexta etapa, vuelve a comenzar el ciclo.

3.1 Conocer la situación actual

En primer lugar, se deben realizar diversos análisis teniendo en cuenta aspectos técnicos, organizativos, regulatorios y normativos. Es la fase de mayor importancia y complejidad, debido a que participan múltiples personas y a la gran importancia que tiene la fiabilidad, completitud y actualidad de la información de la organización para poder evaluar su situación.

Es primordial que la Dirección apoye y supervise esta etapa, puesto que es necesario calcular los recursos necesarios para llevar a cabo el Plan Director de Seguridad y que esté alineado con la visión estratégica de la empresa.

3.1.1 Acotar y establecer alcance

El alcance de este plan es securizar el Sistema de Control Industrial de la subestación eléctrica propuesta en el apartado “5.6 Infraestructura de partida de la subestación propuesta”.

Para llevar a cabo esta valoración, se sigue el flujo de la Figura 14, designado en la norma IEC 62443-2 [8].

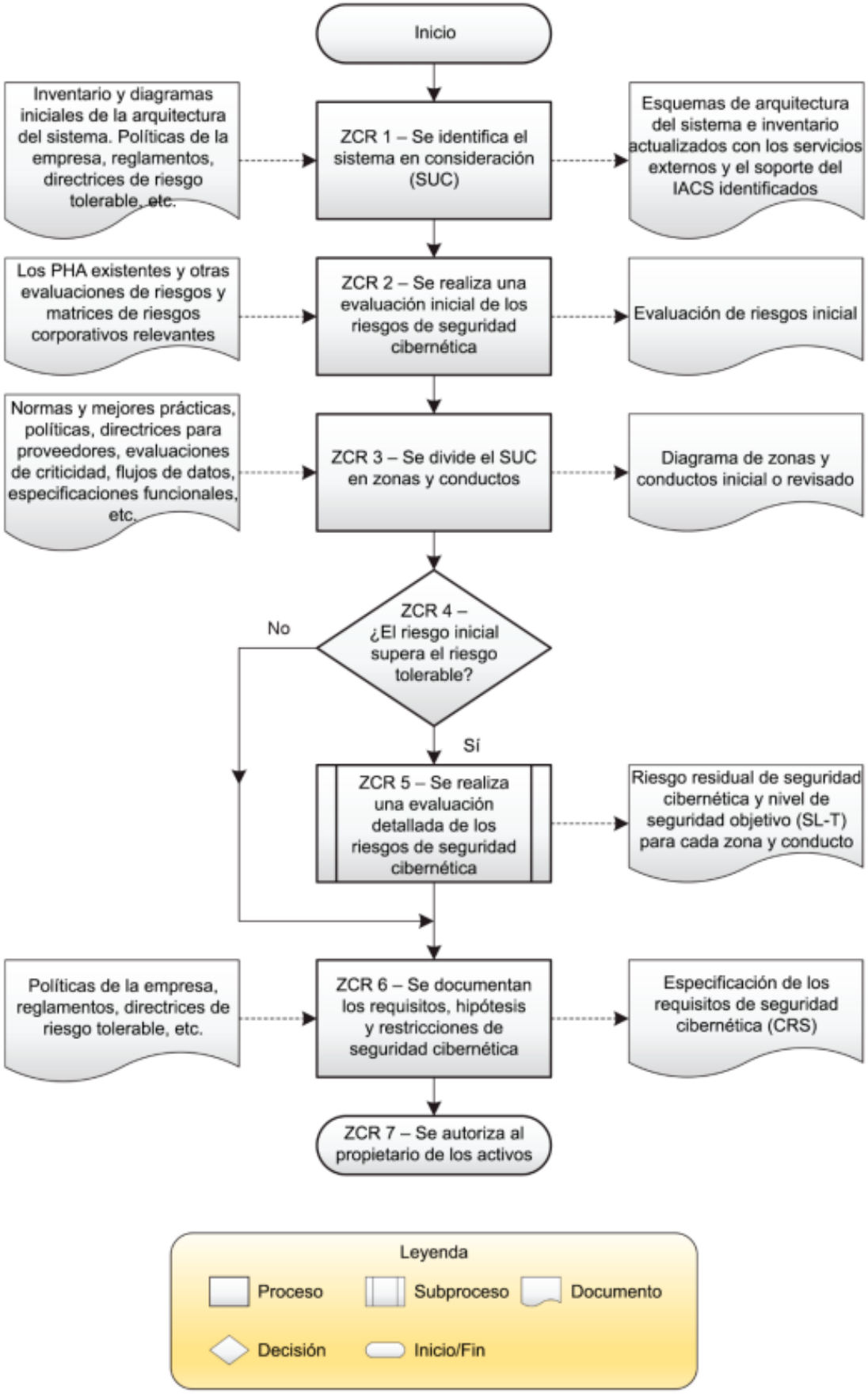

Figura 14. – Diagrama de flujo de trabajo que resume los principales pasos necesarios para establecer zonas y conductos, así como para evaluar el riesgo [8].

Requisitos de zonas y conductos

Se definen los requisitos de zonas y conductos, representados en el flujo de la Figura 14.

- **ZCR 1**. Identificación del sistema en consideración (SUC).

Se debe identificar de manera clara el sistema en consideración, incluyendo la demarcación del perímetro de seguridad y la identificación de todos los puntos de acceso.

- **ZCR 2**. Realización de una evaluación inicial de riesgos de seguridad cibernética.

Se realiza una evaluación de riesgos de seguridad cibernética en el sistema en consideración para poder considerar las condiciones más desfavorables de riesgo de seguridad cibernética que podría afectar al IACS.

- **ZCR 3.1.** Agrupación de los activos y los IACS relacionados en zonas o conductos según el riesgo.

Los grupos se deben fundamentar en los resultados de la evaluación inicial de seguridad cibernética, o en otras reglas, como la función operativa, la criticidad de los activos, la ubicación física o lógica, la organización responsable o el acceso requerido.

- **ZCR 3.2.** Separar los activos de la empresa y del IACS.

Se deben agrupar los activos del IACS en zonas separadas de manera física o lógica de los activos del sistema de negocio o empresarial.

- **ZCR 3.3**. Separar los activos relacionados con la seguridad.

Los activos del IACS que estén relacionados con la seguridad se deben agrupar en zonas que estén separadas física o lógicamente de las zonas con activos no relacionados con la seguridad.

- **ZCR 3.4**. Separar los dispositivos conectados temporalmente.

Los dispositivos que realicen conexiones temporales al sistema en consideración deberían agruparse en una o varias zonas separadas de los activos que estén conectados permanentemente al IACS.

- **ZRC 3.5.** Separar los dispositivos inalmámbricos.

Aquellos dispositivos inalámbricos deben estar en una o más zonas separadas de los dispositivos conectados por cable.

- **ZRC 3.6.** Separar los dispositivos conectados a través de redes externas.

Aquellos dispositivos que se permitan conectar al sistema en consideración a través de redes ajenas, se agruparán en una o más zonas separadas.

- **ZRC 4.1.** Comparación del riesgo inicial con el riesgo tolerable.

El riesgo inicial se debe comparar con el riesgo que es tolerable para la organización. En caso de sobrepasarlo, se deberá realizar una evaluación detallada de los riesgos de seguridad cibernética, como indica la norma [8].

3.1.1.1 Identificación del sistema en consideración

Se debe identificar de manera clara el sistema en consideración (SUC), incluyendo una demarcación clara del perímetro de seguridad y se identifican todos los puntos de acceso al SUC. Esta clasificación de zonas se hace en base al modelo de referencia de Purdue, definido en la norma IEC 62264-1.

En la Tabla 9, se describe en qué zona se sitúan los activos del sistema en consideración. Se presentan las siguientes cinco zonas: DMZ de Internet, Zona empresarial, Zona de Desmilitarización, Interfaces Hombre-Máquina, Dispositivos de Control y Dispositivos de Campo. La Figura 32 del apartado "5.1.1. Segmentación física de la red", puede ayudar a comprender mejor esta tabla.

Tabla 9. Indentificación de zonas y activos.

Num zona	Zonas	Activos
5	**DMZ de Internet**	Servidores web y Servidores de email
4	**Zona empresarial**	Servidores web, Controlador de dominio, Servidores empresariales y Estaciones de trabajo empresariales
3.5	**Zona de Desmilitarización (DMZ)**	Acceso remoto, copia de seguridad del Historian[1], WSUS (Windows Server Update Services), Servidor de Parches de Seguridad y Firewall perimetrales.
3	**Sistemas de Operación**	Servidores de aplicación, servidores de bases de datos, Historian (servicio de software de bases de datos para Control permanente y a largo plazo), Controladores de dominio, Estación de Trabajo del operador de red local y SIEM (Gestor de información y eventos de seguridad)
2	**Interfaces Hombre-Máquina**	HMI (Human Machine Interface) o SCADA (Supervisory Control And Data Adquisition)
1	**Dispositivos de control**	PLC (Controlador Lógico Programable) o RTU (Unidad de Transmisión Remota)
0	**Dispositivos de campo**	Sensores o actuadores

[1] Historian: Es un servicio de software de bases de datos para Control permanente y a largo plazo. Es un componente fundamental del sistema SCADA donde se almacenan logs e informes de los datos históricos de la planta.

Adicionalmente, se han considerado los siguientes grupos de activos para poder describir los escenarios de riesgo más fácilmente, recogidos en la Tabla 10, en conjunto con una descripción, y los responsables de cada conjunto de activos.

Tabla 10. Activos organizados en grupos para describir los escenarios de riesgo.

Activo	Descripción	Responsables
Archivos de proyecto	Son todos aquellos archivos (documentos, planos, copias de seguridad, programas…) están involucrados en un proyecto	Responsable de Seguridad, Re sponsable de Información
Lógica en ejecución en controladores y/o PC SCADA	Se trata de los programas cargados en memoria, en ejecución en los dispositivos de la planta	Responsable de Seguridad, Re sponsable de Información, Propietario del activo donde se encuentra la lógica en ejecución
Equipos, máquinas y/o instalaciones	Engloba los equipos descritos en la tabla anterior, en conjunto a las propias instalaciones de la planta	Responsable de Seguridad, Propietario del activo en cuestión
Materia prima, material en proceso y/o producto terminado	En el caso de la subestación eléctrica, se trata de la producción, conversión, transformación, regulación y distribución de la energía eléctrica	Responsable de Seguridad
Información del proceso y/o de la organización	Información respecto al proceso de producción y a la propia organización	Responsable de Seguridad, Responsable de Información
Red y elementos de la arquitectura de comunicación	Se trata de los switches, routers, firewalls… usados para la arquitectura de red de comunicación	Responsable de Seguridad, Responsable de Información, Técnicos de red
Medio Ambiente	Consiste en el entorno que afecta a los seres vivos del lugar	Responsable de Seguridad, Responsable de medio ambiente
Personal propio y/o de terceros	Son el conjunto de personas que trabajan para la organización de manera interna y externa	Responsable de Seguridad, Responsable de Información
Terceras personas	Son personas ajenas a la organización	Responsable de Seguridad, Responsable de Información

A su vez, pueden existir agentes que están involucrados en los distintos escenarios de riesgo. Dentro de la Tabla 11, se encuentra una descripción de cada tipo de agente.

Tabla 11. Agentes involucrados en los escenarios de riesgo.

Id	Agentes	Descripción
1	**Ciberdelincuentes**	Aquellas personas que buscarán sacar beneficio de estos problemas o fallos de seguridad utilizando para ello distintas técnicas como es la ingeniería social o el malware. [38]
2	**Personal propio y de terceras partes**	Son el conjunto de personas que trabajan para la organización de manera interna y externa. El daño se puede causar de forma voluntaria o involuntaria.
3	**Estados**	Forma de organización política, dotada de poder soberano e independiente, que integra la población de un territorio. [39]
4	**Terroristas**	Personas que practican provocación o mantenimiento en estado de terror a la población, mediante actos que pongan en peligro la vida, la integridad física o la libertad de las personas o la conservación de los bienes. [40]

3.1.2 Responsables de la gestión de los activos

Es importante definir las responsabilidades sobre los activos, para poder hacer un seguimiento de la ejecución de las medidas implantadas. Se han establecido los responsables de los activos en la Tabla 10 del apartado anterior.

Se han definido los siguientes perfiles de responsabilidad sobre los activos [37]:

- Responsable de Seguridad: Es la figura que se encarga de hacer un seguimiento y coordinar las iniciativas en materia de Seguridad de la Información
- Responsable de Información: Es indispensable cuando se trata con información específica gestionada a través de diferentes entornos.
- Responsable de ámbito: Iniciativas en el ámbito lógico, físico, legal y organizativo.
- Técnicos específicos que trabajan con los dispositivos

3.1.3 Evaluación inicial de los riesgos de seguridad cibernética

Para llevar a cabo la evaluación inicial de los riesgos de seguridad cibernética, se consideran doce escenarios de riesgo, sobre los cuales se calculará el riesgo asociado, estudiando el impacto y probabilidad de cada uno de los elementos de riesgo que conlleva cada escenario, y se presentará el nivel de seguridad y madurez del sistema.

3.1.3.1 Escenarios de riesgo

Se realiza el análisis de riesgos de los activos de la planta industrial, siguiendo los siguientes 12 escenarios de riesgo de la referencia "Amenazas y análisis de riesgos en Sistemas de Control Industrial" del Centro Criptológico Nacional [41]:

- ER1: Uso inadecuado de dispositivos portátiles
- ER2: Trabajo de terceros
- ER3: Interconexiones con otras redes
- ER4: Gestión deficiente de copias de seguridad
- ER5: Falta de concienciación del personal
- ER6: Inadecuada gestión de cambios
- ER7: Inexistencia de planes adecuados de gestión de incidentes y continuidad
- ER8: Gestión deficiente de la información
- ER9: Gestión deficiente del software
- ER10: Asignación deficiente de responsabilidades y gestión de la seguridad
- ER11: Gestión deficiente de usuarios y contraseñas
- ER12: Falta de gestión técnica de la seguridad y sistemas

Para cada uno de los escenarios de riesgo se ha rellenado una tabla como la siguiente, indicando los activos y agentes involucrados en el mismo. Adicionalmente, se exponen los factores de riesgo que afectan al escenario y se ha establecido el contexto de este, para una mejor compresión.

Tabla 12. Tabla de ejemplo de evaluación de escenarios de riesgo.

Activos	Agentes
Activos involucrados en el escenario, es decir, los recursos afectados.	Agentes involucrados en el escenario, es decir, un ciberdelincuente interno o externo capaz de afectar la seguridad de los datos [42].
Factores de riesgo	
Es toda circunstancia o situación que aumenta las probabilidades de que el escenario de riesgo acabe provocando un impacto en el sistema.	
Contexto	
Descripción del escenario de riesgo, para facilitar la comprensión del mismo.	

ER1: Uso inadecuado de dispositivos portátiles

Tabla 13. ER1: Uso inadecuado de dispositivos portátiles [41].

Activos	Agentes
• Lógica en ejecución en controladores y/o PC SCADA • Equipos, máquinas y/o instalaciones • Información del proceso y/o de la organización	• Ciberdelincuentes • Personal propio y de terceras partes • Estados • Terroristas
Factores de riesgo	
A. Copias de seguridad de información de la lógica en ejecución en discos duros externos. B. Extracción de información de la red de control con dispositivos USB para la realización de informes. C. Uso de dispositivos USB para el intercambio de información relevante para el proceso productivo (precios de producto, información de proveedores, diagramas de proceso, planos, arquitectura de la red de control, marcas y modelos de equipos en producción, etc.) D. PC portátiles con aplicaciones específicas empleadas en el mantenimiento de equipos de los ICS. E. Existencia de hardware específico de configuración o mantenimiento.	
Contexto	
Es común el uso de dispositivos extraíbles en entornos industriales puesto que es frecuente que las sedes de control no se encuentren conectadas entre sí. No suelen existir procedimientos para el uso, análisis previo y posterior de estos dispositivos, por lo que se introducen una serie de riesgos. Es frecuente que estos dispositivos de almacenamiento se usen en equipos que pueden conectarse a otras redes, lo que puede conllevar a: • Robo de información (hurto de dispositivo) • Conexiones asíncronas a la red del Sistema de Control Industrial, es decir, la comunicación de datos de la red industrial hacia fuera y viceversa Además, es común el uso de estos dispositivos para llevar a cabo copias de seguridad de la lógica de ejecución del sistema de control, lo que puede ocasionar: • Pérdida de información crítica para la continuidad de la operación si el dispositivo se extravía	

ER2: Trabajo de terceros

Tabla 14. ER2: Trabajo de terceros [49].

Activos	Agentes
• Archivos de proyecto/programas • Lógica en ejecución en controladores y/o PC SCADA • Equipos, máquinas y/o instalaciones • Información del proceso y/o de la organización	• Ciberdelincuentes • Personal propio y de terceras partes • Estados • Terroristas
Factores de riesgo	
A. Existencia de conexiones con un módem de radio o celular (tecnologías 2G/ 3G /4G/ CDMA14 o GSM15) en subsistemas de la red de control con o sin conocimiento por parte de la organización. B. Conexión con equipos PC portátiles no revisados al sistema de control. C. Archivos de proyectos o copias de seguridad únicamente en manos de proveedores. D. Existencia de conexiones para mantenimiento remoto de las que no se guarda ningún tipo de registro en el sistema o sobre el que no hay un control de acceso adecuado E. Personal de mantenimiento de terceras empresas al que no se le aplican políticas de seguridad para terceros. F. Equipos conectados a subsistemas del ICS sobre los que la organización no tiene ningún tipo de control o sobre los que no se accede porque son utilizados para el mantenimiento remoto por parte de proveedores.	
Contexto	
• Debido a que el sector industrial requiere un grado de especialización muy alto es frecuente que la organización cuente continuamente con tercereras empresas para llevar a cabo tareas imprescidibles para el correcto funcionamiento del proceso industrial. En muchos casos al ser personal frecuente en las instalaciones es común que no se apliquen sobre ellos las políticas para terceros. • Puede existir información de operación del proceso de las cuales la propia organización no tiene respaldo, solo la empresa tercer que se encargó de proveer dicha parte del sistema. • Pueden haber conexiones remotas para el mantenimiento en el caso de equipos en garantía. A veces incluso los proveedores instalan tecnologías s 2G/ 3G /4G/ CDMA o GSM de los que la organización no tiene si quiera conocimiento. • Deben considerarse las conexiones ocasionales al sistema de control cuando se lleva a cabo un mantenimiento presencial. Los equipos de terceros no suelen revisarse antes de conectarse a la red. • El trabajo de terceros introduce el riesgo de incumplimiento de políticas de seguridad de la información. Debe hacerse un control exhaustivo del modo en que los terceros trabajan con dicha información y la intercambian a su vez con otras personas.	

ER3: Interconexiones con otras redes

Tabla 15. ER3: Interconexiones con otras redes [41].

Activos	Agentes
• Lógica en ejecución en controladores y/o PC SCADA • Equipos, máquinas y/o instalaciones • Información del proceso y/o de la organización • Procesos industriales	• Ciberdelincuentes • Personal propio y de terceras partes • Estados • Terroristas
Factores de riesgo	
A. Segmentación inadecuada de la red corporativa con la red ICS. B. Control de acceso no adecuado en la gestión remota de dispositivos. C. Segmentación inadecuada en el acceso de terceros para el mantenimiento de sistemas. D. Línea independiente en subsistema del proceso sin monitorización por parte de la organización. E. Actualizaciones en la arquitectura de la red de control que no están bien documentadas y que han introducido interconexiones sin ser éstas advertidas. F. Segmentación inadecuada entre los niveles de control y supervisión en la red de control. G. Integración de procesos con socios (partners). H. Uso de redes públicas de comunicación. I. Organizaciones con centros de control centralizados y sistemas con amplia distribución geográfica.	
Contexto	
• Es frecuente encontrar segmentaciones incorrectas entre los niveles de control y supervisión o conexiones que se han introducido al realizar cambios en la arquitectura que no se han revisado convenientemente. • Es común encontrarse interconexiones con otras redes, a menudo desconcidas por los propios operadores del sistema • Pueden existir conexiones remotas por parte de los terceros para el mantenimiento, y en muchos casos a través de líneas independientes con tecnologías 2G/ 3G /4G/ CDMA o GSM. • Estas conexiones carecen de autenticación y no es común que haya firewalls que registren la información de las conexiones que se establecen de manera adecuada	

ER4: Gestión deficiente de copias de seguridad

Tabla 16. ER4: Gestión deficiente de copias de seguridad [41].

Activos	Agentes
• Archivos de proyecto • Personas • Medio ambiente • Procesos industriales • Lógica en ejecución en controladores y/o PC SCADA • Información del proceso y/o de la organización	• Personal propio y de terceras partes
Factores de riesgo	
A. No verificación de las copias de seguridad del ICS. B. Copias no actualizadas de la lógica en ejecución en el ICS C. Inexistencia de copias de seguridad. Dependencia de los archivos que se encuentran en manos proveedor. D. No ejecución de copias de seguridad previas a actualizaciones de cualquier tipo. E. Diversidad de repositorios para copias de seguridad, etiquetado inadecuado de las mismas u otras situaciones que crean confusión en caso de tener que reestablecer una copia. F. Imposibilidad de acceso a la lógica de control en PLC para llevar a cabo copias de seguridad porque el proveedor ha protegido el programa con una contraseña que la organización desconoce. G. Periodos de garantías en los que la organización depende de un proveedor para resolver incidentes en ciertos equipos del ICS.	
Contexto	
La información contenida en las copias de seguridad es crítica. • Su pérdida puede ocasionar problemas en el proceso de producción • Es frecuente que partes del Sistema de Control Industrial se subcontrate a terceros que a su vez se encargan del mantenimiento, es común que en la propia plante no se disponga de los recursos o conocimientos necesarios para restaurar el sistema o alguno de los componentes sin que intervenga un tercero • Idealmente las copias de seguridad deberían ser automáticas aunque en muchos casos no es posible (elementos distribuidos por la planta o no siempre conectados), por lo que deben hacerse de forma manual. • Las copias deben almacenarse identificando la fecha y hora de las mismas y comprobando que se han copiado satisfactoriamente. • Las copias de seguridad deben poder respaldarse • Es frecuente que aquellas copias que se realizan de forma manual se hagan usando soportes extraíbles con los riesgos que ello conlleva, como pérdida de información, no tener un control de accesos adecuado, se modifiquen las copias de seguridad	

ER5: Falta de concienciación del personal

Tabla 17. ER5: Falta de concienciación del personal [41].

Activos	Agentes
• Personas	• Ciberdelincuentes • Estados • Terroristas
Factores de riesgo	
A. Personal del ICS que, por desconocimiento del riesgo que supone, antepone un mantenimiento rápido del sistema a que las conexiones remotas para llevarlo a cabo se realicen de manera segura. B. Desconocimiento de que, si se accede directamente a las comunicaciones entre los dispositivos, hay acciones que se pueden llevar a cabo sobre el ICS aunque el software que se utiliza habitualmente no lo permita. C. Uso inadecuado de los equipos del ICS. D. Publicación de excesiva información sobre la organización en perfiles personales en redes sociales de los empleados. E. No conciencia de la existencia de información pública detallada sobre los propios sistemas (artículos técnicos, casos de éxito de proveedores, etc.) F. Incapacidad para reconocer un incidente y/o desconocimiento de cómo comunicarlo o actuar	
Contexto	
• Desconocimiento por parte del personal del ámbito de la seguridad de la información • Evolución tecnológica ha provocado que en muchas tareas de los operadores intervengan multitud de elementos que introducen riesgos relacionados con las tecnologías de la información y las comunicaciones, como el uso del correo electrónico, intercambio de ficheros a través de la nube, uso de dispositivos de almacenamiento extraíble, etc… • Trabajadores pueden llegar a generar riesgos de diferentes formas, como descargarse archivos infectados con malware, phishing, ingeniería social, etc… • El control sobre la lógica de programación y los enclavamientos asociados ha de ser mucho más fuerte ahora para evitar que personas no autorizadas modifiquen el funcionamiento y provoquen situaciones no deseadas.	

ER6: Inadecuada gestión de cambios

Tabla 18. ER6: Inadecuada gestión de cambios [41].

Activos	Agentes
• Archivos de proyecto • Información del proceso y/o de la organización	• Ciberdelincuentes • Personal propio y de terceras partes • Estados • Terroristas
Factores de riesgo	
A. Actualizaciones de seguridad en equipos de la red de control sin verificar que no se producen incompatibilidades con el software del ICS. B. Cambios en la arquitectura por la introducción de nuevos subsistemas que no se han reflejado en la documentación. C. Políticas de gestión de cambios que no incluyen o excluyen explícitamente del procedimiento modificaciones o actualizaciones de software específico del ICS (lógica de control, SCADA, etc.) D. No se realiza borrado seguro de los equipos del ICS (PLC, HMI20, etc.) tras ser retirados. E. La política de gestión de cambios no incluye la ejecución de copias de seguridad previa a la actualización de cualquier tipo de software de la red de control.	
Contexto	
• En la gestión de cambios es común que no se tengan en cuenta los elementos software. • Deben tenerse en cuenta los sistemas operativos, actialzaciones de PC, software de los ICS (lógica de ejecución en el proceso, pantallas de SCADA, sistemas operativos de PLC, HMI, etc…). • Debe asegurarse de que antes de llevar a cabo un cambio se hagan las evaluaciones pertinentes para asegurarse que las modificaciones no producirán incompatibilidades • La actualización de un sistema operativo y el software que se utiliza en los dispositivos industriales tiene un coste muy elevado, adquirir nuevas licencias suele requerir grandes inversiones e incluso puede darse el caso de que no existan versiones para un sistema operativo concreto y el mantenimiento que hacen los desarrolladores no siempre es el adecuado. • En ciertos cambios intervienen terceras empresas subcontratadas especialistas y se pueden generar residuos que deben ser vorrados de manera segura. • Es frecuente que, tras llevas a cabo ciertas modificaciones no se actualice la documentación asociada a planos, arquitecturas de red, diagramas de proceso, etc… • La gestión de cambios debe incluir copias de seguridad que permitan revertir la modificación en caso de que surja alguna incompatibilidad	

ER7: Inexistencia de planes adecuados de gestión de incidentes y continuidad

Tabla 19. ER7: Inexistencia de planes adecuados de gestión de incidentes y continuidad [41].

Activos	Agentes
• Equipos, máquinas y/o instalaciones • Materia prima, material en proceso y/o producto terminado • Medio Ambiente • Personal propio y/o de terceros • Terceras personas	• Ciberdelincuentes • Estados • Terroristas
Factores de riesgo	
A. Organizaciones sin gestión de la ciberseguridad o donde el alcance no incluye los ICS. B. Planes de emergencias que no contemplan un incidente de ciberseguridad como causa de la situación de emergencia	
Contexto	
• En los procedimientos de gestión de incidentes y continuidad industriales es común que no contemplen ciberataques	

ER8: Gestión deficiente de la información

Tabla 20. ER8: Gestión deficiente de la información [41].

Activos	Agentes
• Archivos de proyecto • Lógica en ejecución en controladores y/o PC SCADA • Información del proceso y/o de la organización	• Ciberdelincuentes • Personal propio y de terceras partes • Estados • Terroristas
Factores de riesgo	
A. En los pliegos de condiciones técnicas se proporciona excesiva información sobre el ICS (pantallas del SCADA y ubicaciones de instalaciones, etc.) B. La información que se comparte con los proveedores se envía en claro a través de correo electrónico o se utilizan plataformas no verificadas por la organización. C. Se proporciona a través de internet, para hacer publicidad de la organización, información excesiva de una planta en producción: detalles del proceso, proveedores, ubicaciones de equipos, respaldos existentes, etc. D. Obligación legal de publicar cierta información E. Los proveedores utilizan el nombre de la organización para mostrar casos de éxito (proporcionando de este modo información sobre protocolos o equipos utilizados en el proceso). F. Existe documentación sobre el proceso o las instalaciones distribuida por los equipos de la planta. G. No se clasifican ni se marcan los documentos relativos al ICS.	
Contexto	
• A veces, no existen normas para el marcado y clasificación adecuadas de los documentos de modo que se sepa quién debe acceder a cierta información y cuál debe ser el nivel de publicidad de esta. • Es frecuente que no existan políticas adecuadas para el intercambio de información entre departamentos o con agentes externos a la organización (subcontratas o proveedores). • Con frecuencia la propia organización pone a disposición pública excesiva información sobre los sistemas de control, como en pliegos de contratación del sector público. A menudo incluyen detalladas explicaciones del proceso que lleva a cabo el sistema de control, ubicación geográfica de las instalaciones, equipos con marcas y modelos utilizados o capturas de pantallas del sistema SCADA. • Puede ocurrir con documentos que por requerimiento legal han de ser públicos, como una autorización ambiental integrada.	

ER9: Gestión deficiente del software

Tabla 21. ER9: Gestión deficiente del software [41].

Activos	Agentes
• PC, controladores y otro hardware	• Ciberdelincuentes • Personal propio y de terceras partes • Estados • Terroristas
Factores de riesgo	
A. No se actualiza el software con parches de seguridad en equipos del ICS como consecuencia, por ejemplo, de la dificultad de hacerlo en sistemas distribuidos en un territorio amplio. B. No existe un inventario de programas y versiones de cada equipo. C. No se verifica previamente que las actualizaciones de sistema operativo (SO) en equipos que se utilizan en la red de control (tanto en el proceso como en mantenimiento) pueden generar incompatibilidades con software crítico para el funcionamiento del proceso. D. No se revisan de manera periódica los equipos en búsqueda de documentación o software no pertinente. E. No se llevan a cabo copias de seguridad antes de cualquier actualización de software.	
Contexto	
• No es una práctica habitual tener un inventario de software para cada equipo dentro del ICS • Es frecuente encontrar programas instalados para una necesidad puntual, no verificados y se dejan indefinidamente. • Deben verificarse los programas y actualizaciones antes de instalarse • Habitualmente las redes de control no se conectan a internet, y por tanto no se actualizan los antivirus, lo cual disminuye su efectividad. Es importante verificar el software de manera continua.	

ER10: Asignación deficiente de responsabilidades y gestión de la seguridad

Tabla 22. ER10: Asignación deficiente de responsabilidades y gestión de la seguridad [41].

Activos	Agentes
• Lógica en ejecución en controladores y/o PC SCADA • Información del proceso y/o de la organización	• Ciberdelincuentes • Personal propio y de terceras partes • Estados • Terroristas
Factores de riesgo	
A. No existe un responsable de ciberseguridad de los ICS. B. No existen propietarios de los activos del ICS. C. No existen procedimientos para la transferencia de propiedad de activos D. No existen procedimientos para el borrado seguro de equipos de sistema de control	
Contexto	
• Existen responsables de la seguridad física y de "safety" o medio ambiente. Pero rara vez existe un responsable de la seguridad de la información • Por tanto es común que no se aplique ninguna política de seguridad de la información • Es común que los activos no tengan asignados un propietario • Con frecuencia no existen procedimientos claros para la gestión de la información almacenada	

ER11: Gestión deficiente de usuarios y contraseñas

Tabla 23. ER11: Gestión deficiente de usuarios y contraseñas [41].

Activos	Agentes
• Lógica en ejecución en controladores y/o PC SCADA • Información del proceso y/o de la organización • Procesos industriales	• Ciberdelincuentes • Personal propio y de terceras partes • Estados • Terroristas
Factores de riesgo	
A. No se renuevan las contraseñas del ICS. B. Se utilizan usuarios y contraseñas comunes en todas las instalaciones que son análogas. C. No existe control de acceso en los equipos que contienen lógica en ejecución del proceso D. No existe control de acceso en los equipos que son responsables de la ejecución y restauración de copias de seguridad. E. Los operadores usan usuarios genéricos en vez de nominales. F. Existen equipos de la sala de control o distribuidos por la planta que tienen autologin. G. Existen usuarios y contraseñas escritas junto a los equipos del ICS. H. Existen equipos o software desfasado I. La organización trabaja por turnos	
Contexto	
• Es frecuente que no exista una gestión adecuada de usuarios de los equipos ni de las contraseñas asociadas a los mismos • Es común encontrar contraseñas pegadas en pantallas, poco robustas y fácilmente deducibles o que no se cambian desde el día en que los equipos se instalaron • Es habitual que existan equipos PC con usuarios genéricos compartidos en los que trabajan de manera continuada varios empleados • Algo similar existe en una estación de ingeniería en la sala de control. Generalmente este equipo tiene información crítica de la lógica de control en ejecución e incluso permite realizar cambios y cargarlos al sistema en producción. No es extraño encontrar estos equipos desbloqueados o con usuarios que no son personales	

ER12: Falta de gestión técnica de la seguridad y sistemas

Tabla 24. ER12: Falta de gestión técnica de la seguridad y sistemas [41].

Activos	Agentes
• Lógica en ejecución en controladores y/o PC SCADA • Equipos, máquinas y/o instalaciones • Información del proceso y/o de la organización • Medio Ambiente • Personal propio y/o de terceros • Terceras personas	• Ciberdelincuentes • Personal propio y de terceras partes • Estados • Terroristas
Factores de riesgo	
A. No se lleva a cabo ningún tipo del control sobre el tráfico de la red del ICS. B. Se desconocen las vulnerabilidades o no se lleva a cabo su parcheo en los equipos del ICS. C. No se gestionan adecuadamente o no existen cortafuegos (firewalls) en la red de control. D. Las reglas de los cortafuegos no son adecuadas. E. La segmentación de la red de control y la red corporativa es deficiente. F. No se hace uso de protocolos cifrados en la red de control. G. No se hacen evaluaciones periódicas de ciberseguridad.	
Contexto	
• En la industria la vida útil de los equipos es muy elevada, por lo que es frecuente que equipos de cierta antigüedad no fueran concebidos para usar protocolos cifrados. • Debido a la criticidad, en muchos sistemas los retrasos no son admisibles, y los protocolos cifrados introducen un cierto retraso. • Cambiar los protocolos de comunicaciones en muchos casos supone cambiar los equipos con el coste económico que ello conlleva. • No es frecuente que se guarden y revisen los logs de los diferentes equipos del sistema ni se instalen cortafuegos, ni que se establezcan configuraciones adecuadas en los mismos y es común encontrar segmentaciones deficientes en la red de control. • No se suelen llevar a cabo revisiones de la arquitectura ni auditorías peródicas de las mismas. • Los Sistemas de Detección de Intrusiones usan reglas específicas para cada uno de los protocolos de comunicación y es necesario tener un conocimiento profundo del proceso y del modo en que los equipos diferentes interactúan entre sí.	

3.1.3.2 Cálculo del riesgo de cada uno de los escenarios

En primer lugar, se presenta la Tabla 25, donde se muestra el impacto en los 5 niveles definidos, clasificados en seis criterios de impacto diferentes en la planta industrial, tomando de referencia el artículo [43] y [44].

Tabla 25. Impacto del riesgo en una planta industrial.

5 Catastrófico	Grave efecto adverso en la confidencialidad de la información	Grave efecto adverso en la integridad de la información	Grave efecto adverso en la disponibilidad del sistema n	Pérdidas mayores	Múltiples fatalidades	Consecuencias medio ambientales a largo plazo	Infraestructura crítica internacional afectada	Impacto internacional Reacción mediática extensiva	Pérdidas económicas catastróficas. Imposibilidad de hacer frente al incidente		
4 Mayor	Serio efecto adverso en la confidencialidad de la información	Serio efecto adverso en la integridad de la información	Serio efecto adverso en la disponibilidad del sistema	Pérdidas parciales	Incapacidad permanente	Contaminación significativa	Infraestructura crítica nacional afectada	Impacto nacional. Reacción mediática adversa	Pérdidas económicas adversas. Se debe cerrar la planta o un conjunto de plantas		
3 Moderado	Algún efecto adverso en la confidencialidad de la información	Algún efecto adverso en la integridad de la información	Algún efecto adverso en la disponibilidad del sistema	Efecto local	Daño salud mayor	Contaminación moderada	Efecto local pero no en infraestructura crítica	Impacto considerable. Conocimiento público regional	Se debe hacer un desembolso considerable de capital, pero se consigue reactivar el servicio		
2 Menor	Efecto adverso limitado en la confidencialidad de la información	Efecto adverso limitado en la integridad de la información	Efecto adverso limitado en la disponibilidad del sistema	Efecto menor	Accidente reportado con enfermedad o tratamiento médico	Exceso de contaminación según normativa, pero sin consecuencias en el medio ambiente	Infraestructura esencial no afectada	Impacto limitado. Algo de conocimiento público	Se debe hacer un desembolso de capital menor, pero se consigue reactivar el servicio con normalidad		
1 Insignificante	Efecto insignificante en la confidencialidad de la información	Efecto insignificante en la integridad de la información	Efecto insignificante en la disponibilidad del sistema	Efecto ligero	Accidente reportado sin enfermedad o tratamiento médico	Exceso de contaminación limitada y temporal sin consecuencias legales	Infraestructura complementaria no afectada	Impacto ligero, algo de sensibilización	El desembolso de capital que se debe hacer es ninguno o insignificante		
Confidencialidad La divulgación de información no autorizada puede causar…	**Integridad** La modificación o destrucción de información no autorizada puede causar…	**Disponibilidad** La interrupción de acceso o uso de informacińon puede causar…	**Activos**	**Salud**	**Seguridad**	**Entorno**	**Servicio**	**Reputación**	**Económico**		

En la Tabla 26, se presenta la probabilidad del riesgo en 5 niveles diferentes, en función de la Descubribilidad, Explotabilidad y Reproducibilidad de la vulnerabilidad. Se ha usado como referencia [44].

Tabla 26. Probabilidad del riesgo en una planta industrial.

5 Altamente probable	1. Buscando buscando en información pública 2. Desde redes externas	1. Sin derechos de acceso al objetivo 2. Herramientas públicas disponibles sin conocimiento técnico	- Se puede repetir sin ninguna configuración específica o condición - Se puede repetir a voluntad sin ninguna personalización de los exploits[2] públicos
4 Probable	1. Sondeando al objetivo 2. Desde redes adyacentes, subredes o segmentos de red	1. Requisitos de acceso restringidos al objetivo 2. Herramientas públicas disponibles con conocimiento técnico básico	- Se puede repetir con cierta configuración en el objetivo - Se puede repetir con una mínima personalización de los exploits públicos
3 Posible	1. Examinando las respuestas del objetivo, comportamiento y comunicaciones 2. Desde la misma subred o segmento	1. Requisitos de acceso con privilegios 2. Herramientas disponibles públicamente que requieren conocimientos técnicos medios	- Se puede repetir dada una cierta condición predecible - Se puede repetir con personalización objetiva al objetivo
2 Improbable	1. Interactuando con una configuración similar del objetivo 2. Acceso local lógico	1. Requisitos de acceso con privilegios 2. Herramientas disponibles publicamniente que puedan requerir conocimientos técnicos avanzados y puede requerir de múlitples exploits	- Se puede repetir dada una circunstancia aleatoria - Se puede repetir teóricamente con exploits PoC[3]
1 Excepcional	1. Estudiando el código fuente, data sheets o planos. 2. Requiere acceso físico	1. Con privilegios de acceso elevados y multi-factor de autenticacaión 2. Especializadas que requieren de conocimiento técnico experto y múltiples exploits	- No se puede reproducir en el objetivo - Se puede reproducit con un exploit específico no publicado en el objetivo
	Descubribilidad La vulnerabilidad del objetivo 1. Se puede descubrir … 2. Se puede descubrir y atacar …	**Explotabilidad** El ataque 1. Se puede realizar con requisitos de acceso 2. Herramientas	**Reproducibilidad** El ataque

[2] Exploit: Es un script o fragmento de datos que aprovecha una vulnerabilidad para atacar un sistema.
[3] PoC: Proof Of Concept. Se tratan de pruebas de concepto, de exploits.

Para comprender mejor cómo se ha llevado a cabo el análisis del impacto y probabilidad de cada uno de los elementos de los escenarios de riesgo, se propone el ejemplo, del escenario de riesgo "ER2: Trabajo de terceros", en el factor de riesgo "B. Conexión con equipos PC portátiles no revisados al sistema de control". Para determinar el valor del impacto para dicho factor de riesgo, se toma el mayor número obtenido para cada uno de los ámbitos, y del mismo modo para la probabilidad.

- Evaluar el **impacto** del riesgo en función de 6 ámbitos diferentes, desde insignificante hasta catastrófico.

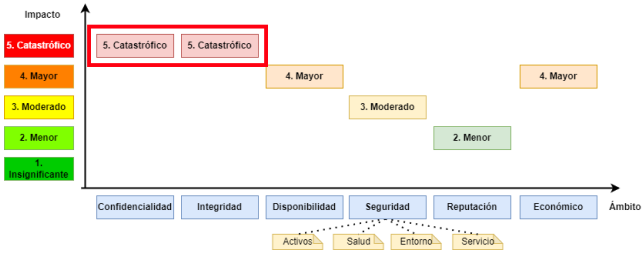

Figura 15. Impacto del riesgo en función de 6 ámbitos diferentes para ER2.B.

- Evaluar la **probabilidad** de que ocurra el riesgo en función de 3 factores diferentes, desde excepcional hasta altamente probable.

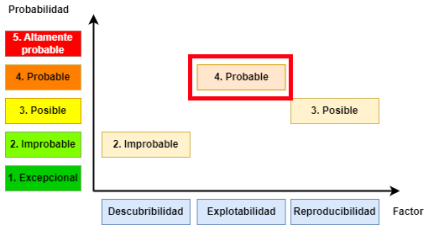

Figura 16. Probabilidad del riesgo en función de 3 factores diferentes para ER2.B.

Para el cálculo del riesgo se ha hecho uso de la siguiente fórmula:

Ecuación 1. Cálculo del riesgo.

$$Riesgo = Impacto \times Probabilidad$$

En la Tabla 27, se presentan los distintos Escenarios de Riesgos ubicados en la matriz de riesgos en función de su probabilidad e impacto, que se estudiaran uno a uno en este apartado.

Tabla 27. Matriz de riesgos [4].

	Impacto				
Probabilidad	**5 Catastrófico**	**4 Mayor**	**3 Moderado**	**2 Menor**	**1 Insignificante**
5 Altamente probable	ER12		15 (Riesgo Alto)	10 (Riesgo Medio)	5 (Riesgo Medio Bajo)
4 Probable	ER3	ER2	ER5	8 (Riesgo Medio)	4 (Riesgo Medio Bajo)
3 Posible	ER7	ER11 ER8	ER4	6 (Riesgo Medio)	3 (Riesgo Medio Bajo)
2 Improbable	10 (Riesgo Medio)	ER10 ER9	ER1 ER6	4 (Riesgo Medio Bajo)	2 (Riesgo Bajo)
1 Excepcional	5 (Riesgo Medio Bajo)	4 (Riesgo Medio Bajo)	3 (Riesgo Medio Bajo)	2 (Riesgo Bajo)	1 (Riesgo Bajo)

[4] El riesgo se divide según la siguiente escala: 25-20 Muy Alto, 19-15 Alto, 14-6 Medio, 5-3 Medio Bajo, 2-0 Bajo

Siguiendo la categorización del Impacto y de la Probabilidad mostradas en las tablas anteriores, se hace una estimación del riesgo, mediante juicio de expertos para cada uno de los elementos de riesgo de cada escenario. Se ha tomado en todo caso, el valor más restrictivo del impacto y probabilidad de cada una de las categorías, es decir, si para un elemento de riesgo el impacto en cuanto a Confidencialidad es Moderado (3), pero en cuanto a Reputación es Catastrófico (5), se toma este último valor, calificándolo como Catastrófico (5).

Tabla 28. Estimación del riesgo de cada uno de los escenarios ER1 y ER2.

Escenario	Elemento de riesgo	Impacto	Probabilidad	Riesgo	RMR[5]
ER1: Uso inadecuado de dispositivos portátiles	A. Copias de seguridad de información de la lógica en ejecución en discos duros externos.	3	3	9	**6,6**
	B. Extracción de información de la red de control con dispositivos USB para la realización de informes.	3	3	9	
	C. Uso de dispositivos USB para el intercambio de información relevante para el proceso productivo	3	3	9	
	D. PC portátiles con aplicaciones específicas empleadas en el mantenimiento de equipos de los ICS.	3	1	3	
	E. Existencia de hardware específico de configuración o mantenimiento.	3	1	3	
ER2: Trabajo de terceros	A. Existencia de conexiones con un módem de radio o celular en subsistemas de la red de control con o sin conocimiento por parte de la organización.	5	3	15	**17,83**
	B. Conexión con equipos PC portátiles no revisados al sistema de control.	5	4	20	
	C. Archivos de proyectos o copias de seguridad únicamente en manos de proveedores.	5	4	20	
	D. Existencia de conexiones para mantenimiento remoto de las que no se guarda ningún tipo de registro en el sistema o sobre el que no hay un control de acceso adecuado	4	5	20	
	E. Personal de mantenimiento de terceras empresas al que no se le aplican políticas de seguridad para terceros.	4	4	16	
	F. Equipos conectados a subsistemas del ICS sobre los que la organización no tiene ningún tipo de control o sobre los que no se accede porque son utilizados para el mantenimiento remoto por parte de proveedores.	4	4	16	

[5] RMR – Riesgo medio del Escenario de Riesgo

Tabla 29. Estimación del riesgo de cada uno de los escenarios ER3 y ER4.

Escenario	Elemento de riesgo	Impacto	Probabilidad	Riesgo	RMR
ER3: Interconexiones con otras redes	A. Segmentación inadecuada de la red corporativa con la red ICS.	5	5	25	**21,67**
	B. Control de acceso no adecuado en la gestión remota de dispositivos.	5	5	25	
	C. Segmentación inadecuada en el acceso de terceros para el mantenimiento de sistemas.	5	4	20	
	D. Línea independiente en subsistema del proceso sin monitorización por parte de la organización.	5	4	20	
	E. Actualizaciones en la arquitectura de la red de control que no están bien documentadas y que han introducido interconexiones sin ser éstas advertidas.	5	3	15	
	F. Segmentación inadecuada entre los niveles de control y supervisión en la red de control.	5	4	20	
	G. Integración de procesos con socios (partners).	5	5	25	
	H. Uso de redes públicas de comunicación.	5	5	25	
	I. Organizaciones con centros de control centralizados y sistemas con amplia distribución geográfica.	5	4	20	
ER4: Gestión deficiente de copias de seguridad	A. No verificación de las copias de seguridad del ICS.	3	2	6	**13**
	B. Copias no actualizadas de la lógica en ejecución en el ICS	3	2	6	
	C. Inexistencia de copias de seguridad. Dependencia de los archivos que se encuentran en manos proveedor.	5	5	25	
	D. No ejecución de copias de seguridad previas a actualizaciones de cualquier tipo.	4	3	12	
	E. Diversidad de repositorios para copias de seguridad, etiquetado inadecuado de las mismas u otras situaciones que crean confusión en caso de tener que reestablecer una copia.	2	1	2	
	F. Imposibilidad de acceso a la lógica de control en PLC para llevar a cabo copias de seguridad porque el proveedor ha protegido el programa con una contraseña que la organización desconoce.	5	4	20	
	G. Periodos de garantías en los que la organización depende de un proveedor para resolver incidentes en ciertos equipos del ICS.	5	4	20	

Tabla 30. Estimación del riesgo de cada uno de los escenarios ER5 y ER6.

Escenario	Elemento de riesgo	Impacto	Probabilidad	Riesgo	RMR
ER5: Falta de concienciación del personal	A. Personal del ICS que, por desconocimiento del riesgo que supone, antepone un mantenimiento rápido del sistema a que las conexiones remotas para llevarlo a cabo se realicen de manera segura.	3	2	6	**15,83**
	B. Desconocimiento de que, si se accede directamente a las comunicaciones entre los dispositivos, hay acciones que se pueden llevar a cabo sobre el ICS aunque el software que se utiliza habitualmente no lo permita.	2	2	4	
	C. Uso inadecuado de los equipos del ICS.	5	4	20	
	D. Publicación de excesiva información sobre la organización en perfiles personales en redes sociales de los empleados.	5	5	25	
	E. No conciencia de la existencia de información pública detallada sobre los propios sistemas (artículos técnicos, casos de éxito de proveedores, etc.)	5	5	25	
	F. Incapacidad para reconocer un incidente y/o desconocimiento de cómo comunicarlo o actuar	3	5	15	
ER6: Inadecuada gestión de cambios	A. Actualizaciones de seguridad en equipos de la red de control sin verificar que no se producen incompatibilidades con el software del ICS.	4	1	4	**6,4**
	B. Cambios en la arquitectura por la introducción de nuevos subsistemas que no se han reflejado en la documentación.	4	1	4	
	C. Políticas de gestión de cambios que no incluyen o excluyen explícitamente del procedimiento modificaciones o actualizaciones de software específico del ICS (lógica de control, SCADA, etc.)	3	1	3	
	D. No se realiza borrado seguro de los equipos del ICS (PLC, HMI20, etc.) tras ser retirados.	4	3	12	
	E. La política de gestión de cambios no incluye la ejecución de copias de seguridad previa a la actualización de cualquier tipo de software de la red de control.	3	3	9	

Tabla 31. Estimación del riesgo de cada uno de los escenarios ER7 y ER8.

Escenario	Elemento de riesgo	Impacto	Probabilidad	Riesgo	RMR
ER7: Inexistencia de planes adecuados de gestión de incidentes y continuidad	A. Organizaciones sin gestión de la ciberseguridad o donde el alcance no incluye los ICS.	5	3	15	**15**
	B. Planes de emergencias que no contemplan un incidente de ciberseguridad como causa de la situación de emergencia	5	3	15	
ER8: Gestión deficiente de la información	A. En los pliegos de condiciones técnicas se proporciona excesiva información sobre el ICS (pantallas del SCADA y ubicaciones de instalaciones, etc.)	5	4	20	**13,86**
	B. La información que se comparte con los proveedores se envía en claro a través de correo electrónico o se utilizan plataformas no verificadas por la organización.	5	4	20	
	C. Se proporciona a través de internet, para hacer publicidad de la organización, información excesiva de una planta en producción: detalles del proceso, proveedores, ubicaciones de equipos, respaldos existentes, etc.	5	3	15	
	D. Obligación legal de publicar cierta información	5	3	15	
	E. Los proveedores utilizan el nombre de la organización para mostrar casos de éxito (proporcionando de este modo información sobre protocolos o equipos utilizados en el proceso).	3	4	12	
	F. Existe documentación sobre el proceso o las instalaciones distribuida por los equipos de la planta.	3	2	6	
	G. No se clasifican ni se marcan los documentos relativos al ICS.	3	3	9	

Tabla 32. Estimación del riesgo de cada uno de los escenarios ER9 y ER10.

Escenario	Elemento de riesgo	Impacto	Probabilidad	Riesgo	RMR
ER9: Gestión deficiente del software	A. No se actualiza el software con parches de seguridad en equipos del ICS como consecuencia, por ejemplo, de la dificultad de hacerlo en sistemas distribuidos en un territorio amplio.	5	5	25	**13,2**
	B. No existe un inventario de programas y versiones de cada equipo.	3	1	3	
	C. No se verifica previamente que las actualizaciones de sistema operativo (SO) en equipos que se utilizan en la red de control (tanto en el proceso como en mantenimiento) pueden generar incompatibilidades con software crítico para el funcionamiento del proceso.	5	3	15	
	D. No se revisan de manera periódica los equipos en búsqueda de documentación o software no pertinente.	5	3	15	
	E. No se llevan a cabo copias de seguridad antes de cualquier actualización de software.	4	2	8	
ER10: Asignación deficiente de responsabilidades y gestión de la seguridad	A. No existe un responsable de ciberseguridad de los ICS.	5	4	20	**13,5**
	B. No existen propietarios de los activos del ICS.	4	3	12	
	C. No existen procedimientos para la transferencia de propiedad de activos	4	3	12	
	D. No existen procedimientos para el borrado seguro de equipos de sistema de control	5	2	10	

Tabla 33. Estimación del riesgo de cada uno de los escenarios ER11 y ER12.

Escenario	Elemento de riesgo	Impacto	Probabilidad	Riesgo	RMR
ER11: Gestión deficiente de usuarios y contraseñas	A. No se renuevan las contraseñas del ICS.	5	3	15	**17,11**
	B. Se utilizan usuarios y contraseñas comunes en todas las instalaciones que son análogas.	5	3	15	
	C. No existe control de acceso en los equipos que contienen lógica en ejecución del proceso	5	4	20	
	D. No existe control de acceso en los equipos que son responsables de la ejecución y restauración de copias de seguridad.	5	4	20	
	E. Los operadores usan usuarios genéricos en vez de nominales.	5	3	15	
	F. Existen equipos de la sala de control o distribuidos por la planta que tienen autologin.	5	4	20	
	G. Existen usuarios y contraseñas escritas junto a los equipos del ICS.	5	3	15	
	H. Existen equipos o software desfasado	5	5	25	
	I. La organización trabaja por turnos	3	3	9	
ER12: Falta de gestión técnica de la seguridad y sistemas	A. No se lleva a cabo ningún tipo del control sobre el tráfico de la red del ICS.	5	5	25	**25**
	B. Se desconocen las vulnerabilidades o no se lleva a cabo su parcheo en los equipos del ICS.	5	5	25	
	C. No se gestionan adecuadamente o no existen cortafuegos (firewalls) en la red de control.	5	5	25	
	D. Las reglas de los cortafuegos no son adecuadas.	5	5	25	
	E. La segmentación de la red de control y la red corporativa es deficiente.	5	5	25	
	F. No se hace uso de protocolos cifrados en la red de control.	5	5	25	
	G. No se hacen evaluaciones periódicas de ciberseguridad.	5	5	25	

Mediante la siguiente representación, se puede observar el riesgo que conlleva cada uno de los escenarios de riesgo, desde el ER1 hasta el ER12. El riesgo medio de cada escenario queda representado mediante la línea roja.

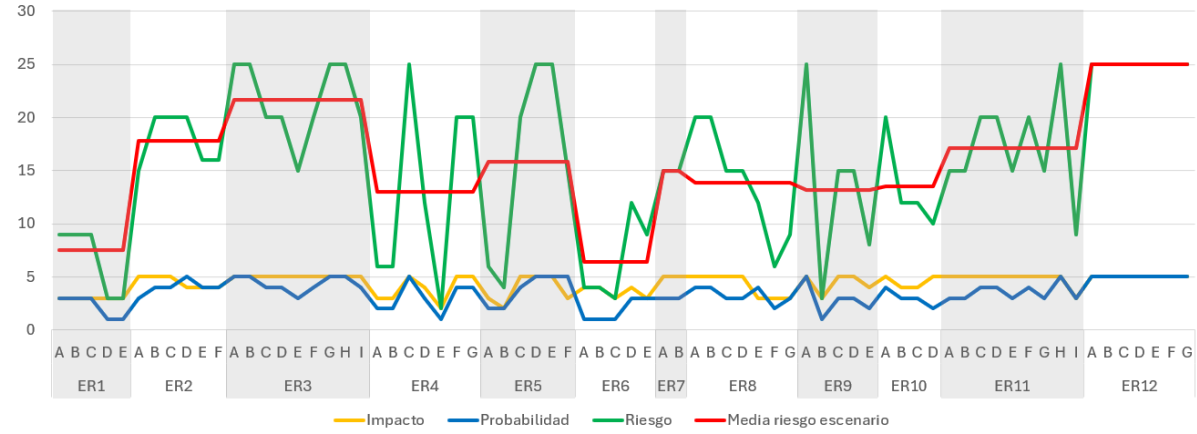

Figura 17. Riesgo de cada uno de los escenarios (ER).

En la Figura 17, se observa como los escenarios de riesgo ER2, ER3 y ER12 son los que más riesgo conllevan. Se han tomado las medidas de mitigación de riesgos (MR) involucradas para cada uno de los escenarios de riesgo, y se han organizado en función de cuales son aquellas que afectan al mayor número de escenarios de riesgo. Con el cómputo del riesgo que mitigan las medidas y la cantidad de escenarios de riesgo que involucran se obtienen las medidas más prioritarias: MR3, MR4 y MR7.

Etiquetas de fila	Cuenta de Medidas
MR4	3
MR7	3
MR3	3
MR5	2
MR6	2
MR11	2
MR13	1
MR14	1
MR8	1
MR2	1
MR10	1
Total general	**20**

Figura 18. Priorización de las medidas (MR) con mayor repercusión.

Debido a que mediante este análisis no se tiene en cuenta el riesgo medio que mitigan las medidas y el coste temporal de implatarlas, en el apartado “3.4 Clasificación y priorización”, se ha realizado otro análisis, que sí considera estos factores. Se calcula la prioridad dividiendo el riesgo entre el coste temporal, llegando a la conclusión de que se deben priorizar las mismas medidas: MR3, MR4 y MR7.

Para mitigar los riesgos de seguridad, se toman medidas legales, técnicas u organizativas. La evaluación de los aspectos normativos y de regulación se realizan tomando como referencia el estándar ISA/IEC 62443. En el apartado “4.1.7 Análisis de riesgos”, se presentan una serie de medidas para mitigar los escenarios de riesgo presentados.

3.1.3.3 Nivel de seguridad y madurez

A continuación, se establece el nivel de seguridad y de madurez de partida y el deseado por la organización, siguiendo la norma IEC 62443-3-3 [45], se clasifican en 4 niveles:

- **Niveles de seguridad (SL – Security Level)**: Busca prevenir la filtración de información de manera no autorizada.

    - **SL 1**: Mediante exposición casual
    - **SL 2**: Por una entidad en búsqueda activa, con pocos recursos, habilidades genéricas y baja motivación.
    - **SL 3**: Por una entidad en búsqueda activa, utilizando métodos sofisticados con recursos moderados, habilidades específicas de IACS y motivación moderada.
    - **SL 4**: por una entidad en búsqueda activa, utilizando métodos sofisticados con recursos extensos habilidades específicas de IACS y motivación alta.

    En el apartado "3.1.5 Establecer los objetivos", se presenta el nivel de seguridad de capacidad y objetivo en cada uno de los Requisitos Fundamentales (FR) en base a la norma IEC 62443.

- **Niveles de madurez (ML - Maturity Level)**:

    - **ML 1**: La organización ejecuta los procesos de manera ad-hoc y sin documentar.
    - **ML 2**: La organización tiene la capacidad de gestionar siguiendo unas políticas escritas.
    - **ML 3**: La organización es capaz de ejecutar sus procesos de manera repetible en toda la organización. Los procesos se han empleado repetidamente y existen evidencias que lo respaldan.
    - **ML 4**: Utilizando métricas adecuadas a los procesos, la organización es capaz de controlar la eficacia de los procesos y el desempeño de los productos y demostrar la mejora continua en estas áreas.

    Se parte con un proyecto en el que no se aplica ninguna política de seguridad, por lo que el nivel de madurez inicial sería ML1. Con la implantación del Plan Director de Seguridad, se pretende al menos alcanzar un nivel ML3. El nivel mínimo para poder certificarse en el estándar IEC 62443 es ML2, es decir, que para los distintos ámbitos del ciclo de diseño seguro existan procesos documentados [45].

3.1.4 Análisis de cumplimiento

Para analizar el cumplimiento se debe:

1. Realizar reuniones con el personal de los distintos departamentos para llevar a cabo una evaluación del cumplimiento de los controles de seguridad implantados.
2. Analizar las medidas de control de acceso físico y seguridad medioambiental para cumplir con los estándares y normativa internacionales.
3. Registrar problemas y evidencias en relación con los requisitos de seguridad.
4. Analizar resultados y realizar el modelo de madurez en cada uno de los controles

3.1.5 Establecer los objetivos

Se deben establecer los objetivos para tener el foco en aquellos ámbitos que más lo requieran. A continuación, en base a la norma IEC 62443, se establece el nivel de seguridad para cada uno de los requisitos establecidos, siendo [2]:

- **SL-C (Security Level - Capacity)**: Nivel de seguridad de capacidad, son los niveles de seguridad que pueden proporcionar los componentes o los sistemas cuando se configuran correctamente. Estos niveles expresan que un componente o sistema determinado es capaz de alcanzar los SL objetivos de forma nativa sin emplear contramedidas compensatorias adicionales cuando están configurados e integrados de la manera correcta.
- **SL-T (Security Level - Target)**: Nivel de seguridad objetivo, son el nivel de seguridad que se desea para un sistema determinado. Normalmente, dicho nivel se determina a través de una evaluación de riesgos de un sistema, con la que se establece que este necesita un determinado nivel de seguridad para garantizar un funcionamiento correcto.
- **SL-A (Security Level - Achieved)**: Nivel de seguridad alcanzado. son el nivel de seguridad real para un sistema determinado. Dichos niveles se miden una vez se dispone de un diseño del sistema o cuando el sistema está implantado. Se utilizan para determinar que un sistema de seguridad está cumpliendo los objetivos que se establecieron en un principio en los niveles de seguridad objetivos.

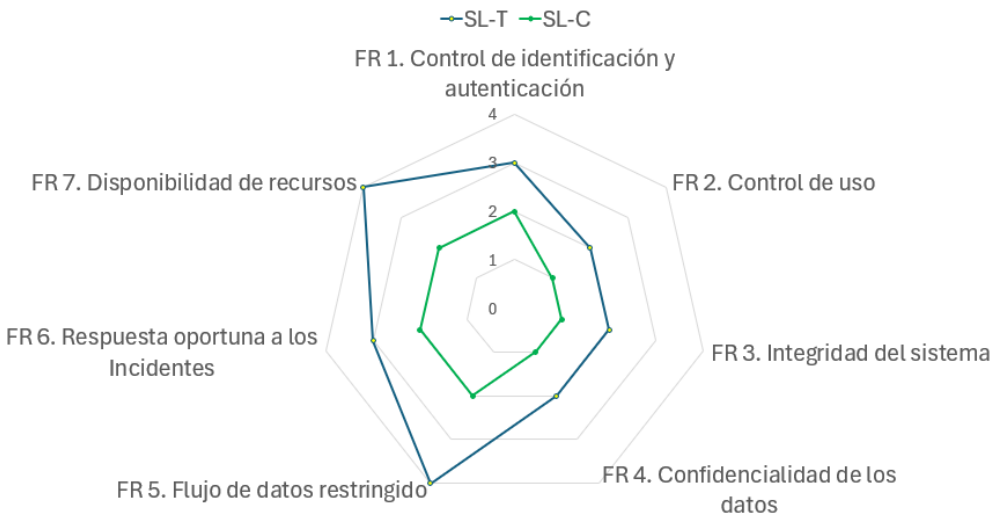

Figura 19. Gráfico ejemplo del resultado de la evaluación [37].

Además, se desea alcanzar un nivel de madurez 4, es decir, la organización ejecuta los procesos utilizando métricas adecuadas a los procesos, la organización es capaz de controlar la eficacia de los procesos y el desempeño de los productos y demostrar la mejora continua en estas áreas.

3.1.6 Análisis técnico de seguridad

El análisis técnico de seguridad queda cubierto mediante la evaluación del grado de implantación y madurez realizado en el apartado anterior.

Es recomendable realizar auditorías técnicas tanto desde el exterior de la organización como desde el interior, para ponernos en el papel de atacantes externos e internos.

3.1.7 Análisis de riesgos

Para llevar a cabo el análisis de riesgos a los que está expuesta la planta industrial, se sigue el siguiente flujo:

Figura 20. Etapas del Análisis de Riesgos [37].

El flujo representado en la Figura 20, es el similar al que está estipulado en la norma IEC 62443 [2], pero mostrado de una manera simplificada. Este flujo se ha desglosado detalladamente, indicando los requisitos de Zonas y Conductos, en el apartado "3.1.1. Acotar y establecer alcance".

1. Identificación de los activos.
2. Valoración de los activos críticos.
3. Principales amenazas.
4. Consecuencias que puede sufrir un activo y probabilidad de que ocurra.
5. Medidas de seguridad existente que reducen la probabilidad o el impacto de las amenazas.
6. Riesgos residuales a los que la organización está expuesta.

Como resultado del análisis de riesgos, se obtiene el conjunto de amenazas a las que la organización está expuesta.

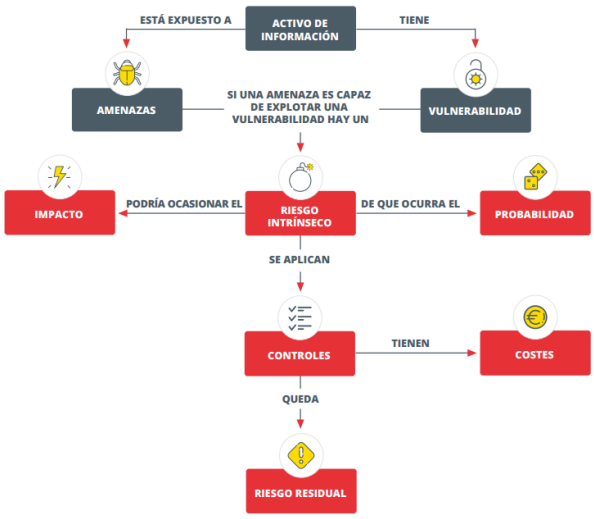

Figura 21. Elementos de la Gestión de la Seguridad de la Información [37].

La Figura 21, representa que un activo está expuesto a amenazas y puede tener vulnerabilidades. En el caso de que una amenaza sea capaz de explotar una vulnerabilidad, habría un riesgo, que tiene una probabilidad de que ocurra y que podría ocasionar un impacto. Para mitigarlo, se aplican controles, los cuales tienen asociados unos costes. Tras aplicar los controles quedaría un riesgo residual. Al final del apartado "3.1.8 Nivel de riesgo aceptable", se profundiza más respecto las medidas de mitigación de riesgo propuestas y el riesgo remanente.

3.1.7.1 Medidas para la mitigación de los riesgos

En el documento publicado por ICS-CERT (Industrial Control Systems Cyber Emergency Response Team) [46], se proponen las siguientes siete medidas para mitigar el riesgo de Sistemas de Control Industrial.

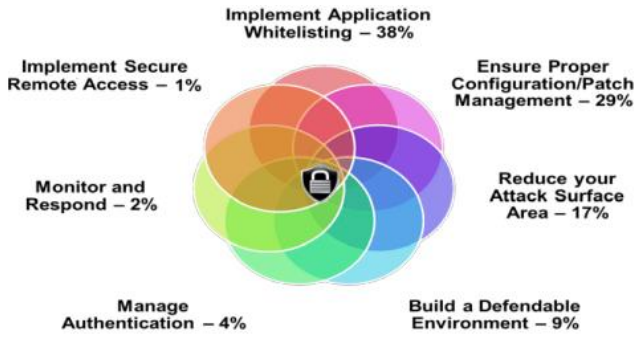

Figura 22. Porcentaje de incidentes potencialmente mitigados por cada estrategia en ICS-CERT FY 2014 y 2015 [46].

A partir de las siete medidas anteriores, se proponen un total de catorce medidas de mitigación de riesgos (MR), para poder cubrir las necesidades de los doce escenarios de riesgo propuestos en el apartado "3.1.3.1. Escenarios de riesgo". Las catorce medidas se han dividido en tres tablas diferentes para presentar la información de manera que estén contenidas dentro del espacio disponible de las páginas del documento.

Tabla 34. Propuesta de medidas de mitigación de riesgos MR1 – MR3.

Medida	Descripción
MR1. Implementación de Listas Blancas sobre aplicaciones (AWL)	Permiten detectar y prevenir la ejecución de malware.
MR2. Configuraciones seguras y gestión de parches	Un Sistema gestor de parches de seguridad y configuración ayudará a mantener los sistemas de control más seguros. • Monitorizar los equipos de la red, para tener en consideración que vulnerabilidades tienen cada uno de ellos para intentar corregirlo lo antes posible, mediante actualizaciones. • Verificar posibles incompatibilidades de las actualizaciones con otro software u otros equipos antes de realizarlas. • Realizar revisiones periódicas en búsqueda de cualquier software no pertinente.
MR3. Reducir la superficie de ataque	Aislar las redes del Sistema de Control Industrial de cualquier otra red no confiable

Tabla 35. Propuesta de medidas de mitigación de riesgos MR4 – MR8.

Medida	Descripción
MR4. Creación de entornos defendibles	Segmentar la red en enclaves lógicos.
MR5. Gestión de la autenticación	Comprometer las credenciales de acceso permite a los adversarios impostar usuarios legítimos dejando un menor rastro de la explotación de vulnerabilidades. Se debe implementar una gestión de la autenticación siguiendo los requisitos de la norma IEC 62443-3-3, "FR 1. Control de identificación y autenticación", con al menos un nivel de seguridad (SL) 3. Prevenir la divulgación no autorizada de información a una entidad que la busca activamente utilizando medios sofisticados con recursos moderados, habilidades específicas de IACS y motivación moderada. • Implementar autenticación multi factor • Reducir los privilegios de los usuarios a los estrictamente necesarios • Políticas de contraseñas complejas • Política de cambio de contraseña al menos cada 90 días
MR6. Implementación de acceso remoto seguro	Algunos adversarios consiguen ganar acceso remoto encontrando accesos escondidos intencionalmente creados por los operadores del sistema. • Eliminar accesos traseros donde sea posible • Limitar todos los accesos a los imprescindibles • Donde sea posible, que los accesos sean de sólo lectura • No permitir conexiones persistentes, siempre con un tiempo limitado • Usar doble factor de autenticación
MR7. Monitorización y respuesta	Establecer programas de monitorización: • Observar el tráfico IP para encontrar posibles comunicaciones sospechosas. • Usar programas en los hosts que permitan detectar software malicioso e intentos de ataque (EDR).
MR8. Plan de concienciación al personal	Consiste en definir un plan de concienciación al personal de la organización, al menos en las siguientes materias: • Gestión de la autenticación: Cómo gestionar sus contraseñas de manera segura. • Gestión de la información: Cómo compartir la información entre los distintos equipos de la planta de manera segura (política de marcado y clasificación de la información adecuadas) y qué información de la organización no deberían compartir con personas ajenas bajo ningún concepto. • Gestión de cambios: Cómo gestionar los cambios realizados en la planta, es decir, documentar los cambios sobre los activos de la planta a lo largo de su vida útil. • Ingeniería social: Concienciar sobre los peligros del phishing. Adicionalmente se podrían hacer campañas de phishing cada cierto tiempo para verificar cuátos y qué empleados son más vulnerables para formarlos y hacer mayor hincapié en ellos. • Gestión de incidentes: Reconocer incidentes, como comunicarlos y actuar.

Tabla 36. Propuesta de medidas de mitigación de riesgos MR9 - MR14.

Medida	Descripción
MR9. Gestión de las copias de seguridad	Crear un plan de gestión de las copias de seguridad, para que a ser posible sean automáticas, estén bien etiquetadas y se verifique que son recuperables. Llevar a cabo las copias de seguridad antes de cualquier actualización.
MR10. Realizar evaluaciones periódicas de ciberseguridad	Realizar auditorias periódicas de ciberseguridad, tanto internas como externas, revisando los propietarios, responsables de los activos y procedimientos. Con el objetivo de la mejora continua del plan de seguridad.
MR11. Desarrollar e implementar una política de seguridad	Desarrollar e implementar una política de seguridad que contenga al menos los siguientes aspectos: • Compromiso de la Dirección. • Utilización del e-mail e Internet. • Utilización de dispositivos móviles. • Aspectos de protección de datos. • Definir un responsable de ciberseguridad. Mantener un listado actualizado de los activos de la red, junto con sus responsables y propietarios. Definir un procedimiento para la transferencia de los activos y borrado de los mismos del sistema. • Política de seguridad de proveedores y terceros
MR12. Mejora en la gestión de incidentes y atención al usuario	Definir, documentar e implantar un proceso para la gestión de los incidentes de seguridad.
MR13. Uso de protocolos de comunicación seguros	Siempre que sea posible utilizar protocolos de comunicación seguros, es decir, que implementen autenticación y cifrado. En su defecto, implementar algún protocolo adicional que implemente estas funcionalidades. De no ser posible ninguna de las dos opciones anteriores, mantener los equipos que se comuniquen usando dicho protocolo inseguro en una red separada, debidamente protegida mediante un firewall.
MR14. Diseño e implantación de un Plan Director de Seguridad Física	El Plan Director de Seguridad Física debería incluir • Sistema de control de accesos (CCAA) • Sistema de cámaras de videovigilancia (CCTV)

3.1.8 Nivel de riesgo aceptable

Antes de medir el nivel de riesgo aceptable, se procede a analizar qué riesgos se pretenden mitigar a través de las medidas propuestas en el apartado anterior. En la siguiente matriz, se presentan en las filas las medidas de mitigación de riesgos (MR), y en las columnas, los escenarios de riesgo (ER).

Con esta matriz se pretende relacionar qué elementos de riesgo (A,B,C…), son mitigados por cada una de las medidas de mitigación de riesgos propuestas. Además, los elementos de riesgo se han subrayado en el color correspondiente a su nivel de riesgo[6].

Tabla 37. Matriz de riesgos a mitigar [7].

ER / MR	ER1	ER2	ER3	ER4	ER5	ER6	ER7	ER8	ER9	ER10	ER11	ER12
MR1									D			
MR2						A			C		H	B
MR3		A B D F	A C D G H I									C D E
MR4		A B D F	A C D G H I									D
MR5		A B E	B								A B C D E F G I	
MR6		A B E	B									
MR7									D			A
MR8	B C D E		E H		Todos	B C D E	Todos	Todos			Todos	
MR9	A			Todos		E			A E			
MR10												G
MR11		A C E	E H	G	C	B C D E		B C	B	Todos		
MR12					Todos		Todos					
MR13												C D F
MR14		E									C D F G	
Riesgos a mitigar	5/5	5/5	9/9	7/7	6/6	5/5	2/2	7/7	5/5	4/4	9/9	7/7

[6] Niveles de riesgo: 25-20 Muy Alto (Rojo), 19-15 Alto (Naranja), 14-6 Medio (Amarillo), 5-3 Medio Bajo (Verde claro), 2-0 Bajo (Verde oscuro).
[7] En cada celda se representan las letras que identifican los riesgos del escenario de riesgo (ER) que se pretende mitigar con la medida de mitigación de riesgos (MR).

Tras la identificar los riesgos, se establece y documenta el nivel de riesgo aceptable, es decir, el umbral que determina que los riesgos deben ser tratados y los riesgos que son asumibles. Además, se realiza un análisis mediante juicio de expertos del riesgo de cada uno de los escenarios tras implantar las medidas de mitigación de riesgos.

En algunos de los casos, las medidas de mitigación de riesgos logran reducir el impacto. Por ejemplo, la medida "MR9. Gestión de las copias de seguridad" logra reducir el impacto tras una pérdida de información por un ataque ransomware, que consiste en encriptar los discos duros de la organización. En otros casos, las medidas de mitigación de riesgos logran reducir la probabilidad de ocurrencia, por ejemplo, la medida "MR8. Plan de concienciación al personal", logra reducir la probabilidad de que un empleado haga click en un enlace malicioso recibido a través de correo electrónico. Obteniéndose así la siguiente tabla comparativa de la estimación del riesgo antes y después de la implantación de las medidas de mitigación.

Tabla 38. Comparativo de la estimación del riesgo antes y después de la implantación de las medidas de mitigación.

Escenario	Riesgo antes de implantar las medidas[8]	Riesgo asumible	Riesgo después de implantar las medidas[9]
ER1: Uso inadecuado de dispositivos portátiles	6,60	5	**3**
ER2: Trabajo de terceros	17,83	2	**1**
ER3: Interconexiones con otras redes	21,67	2	**2**
ER4: Gestión deficiente de copias de seguridad	13,00	6	**3**
ER5: Falta de concienciación del personal	15,83	4	**2**
ER6: Inadecuada gestión de cambios	6,40	6	**3**
ER7: Inexistencia de planes adecuados de gestión de incidentes y continuidad	15,00	3,00	**2**
ER8: Gestión deficiente de la información	13,86	4,00	**3**
ER9: Gestión deficiente del software	13,20	2,00	**2**
ER10: Asignación deficiente de responsabilidades y gestión de la seguridad	13,50	3,00	**3**
ER11: Gestión deficiente de usuarios y contraseñas	17,11	2,00	**2**
ER12: Falta de gestión técnica de la seguridad y sistemas	25,00	2,00	**2**

[8] Riesgo calculado mediante la media aritmética de los riesgos de cada uno de los elementos de riesgo de cada escenario
[9] Estimación a partir de los datos de los riesgos iniciales y las medidas de mitigación propuestas

El riesgo se puede tratar de las siguiente cuatro maneras:

- **Transferir** el riesgo a un tercero, por ejemplo, contratando un seguro o subcontratando algún servicio como auditorías de seguridad o servicio de monitorización.
- **Eliminar** el riesgo, eliminando un proceso que ya no es necesario.
- **Asumir** el riesgo, de manera justificada. Es decir, asumir el coste que tendría disponer de un centro de respaldo en caso de la interrupción del suministro eléctrico puede ser muy elevado y por tanto puede ser necesario asumir el riesgo durante varias horas, a pesar de su impacto.
- **Implantar** medidas para mitigarlo.

Como se puede observar en la Tabla 37, se han tratado de mitigar todos los riesgos implantando medidas para ellos. Y el riesgo residual restante, se asume, debido a que el riesgo cero en ciberseguridad no existe, pero es responsabilidad del Plan Director de Seguridad minimizarlo tanto como sea posible, y de realizar una revisión constante del plan para adaptarse a posibles cambios externos, como nuevos tipos de amenazas o nuevas tecnologías que traen consigo nuevos vectores de ataque.

3.2 Estrategia de la organización

Conocer la estrategia corporativa de la organización implica [37] considerar los proyectos en curso y futuros, qué previsiones hay de crecimiento, qué cambios hay planificados a futuro, etc. Es fundamental tener en cuenta si la organización plantea una estrategia de centralizar los servicios, externalizar los servicios, si forma parte de un grupo empresarial mayor o si va a comenzar la actividad en algún sector diferente al actual, que pueda generar requisitos legales adicionales.

Para llevar a cabo esta fase satisfactoriamente, es recomendable analizar la estrategia de la organización con los responsables de cada uno de los departamentos implicados y la Dirección. De este modo se obtienen dos objetivos, se les hace partícipes del proyecto y se consigue obtener una visión objetiva y global de la estrategia de negocio.

3.3 Definir proyectos e iniciativas

Partiendo de la información recabada hasta este momento, se deben definir las acciones, iniciativas y proyectos necesarios para alcanzar el nivel de seguridad que requiere la organización. Las iniciativas dirigidas a mejorar los métodos de trabajo actuales están recogidas en el apartado "4.1.7.2 Medidas para la mitigación de los riesgos", deben contemplar los controles establecidos por el marco normativo y regulatorio.

Se define la estrategia a seguir y los proyectos más adecuados para gestionar los riesgos por encima del riesgo aceptable. En la medida de lo posible se debe estimar el coste de las iniciativas propuestas en términos temporales y económicos, contemplando los recursos humanos y materiales necesarios a nivel interno y externo.

3.4 Clasificación y priorización

Una vez se hayan identificado las acciones, iniciativas y proyectos, se deben clasificar y priorizar. Es recomendable agrupar las iniciativas o dividir las propuestas para que el conjunto de proyectos que se han definido se pueda llevar a cabo de manera homogénea. Es conveniente organizar los proyectos según el esfuerzo que requieren y a su coste temporal, estableciendo proyectos a corto, medio y largo plazo.

En la Tabla 39, se recoge para cada una de las catorce medidas, el riesgo medio que mitiga, el coste temporal y su prioridad. Para el cálculo de la prioridad se ha dividido el RMR entre el coste temporal de implantar la medida. En un proyecto con un presupuesto, el coste económico también se encontraría dividiendo el RMR. Siendo RMR el riesgo medio de los escenarios en los que la Medida de Mitigación de Riesgos está implicada.

Ecuación 2. Cálculo de la prioridad de las medidas de mitigación de riesgos.

$$Prioridad = \frac{RMR}{Coste}$$

Tabla 39. Priorización y estimación de coste temporal de las medidas de mitigación de riesgos MR1 – MR7.

Medida Mitigción de Riesgos	RMR[10]	Coste temporal	Prioridad[11]
MR1. Implementación de Listas Blancas sobre aplicaciones (AWL)	13,20	**4 semanas** 1 semana configuración + 3 semanas pruebas	**6,6** **Alta**
MR2. Configuraciones seguras y gestión de parches	15,43	**6 semanas** 3 semana configuración + 3 semana pruebas	**5,14** **Media**
MR3. Reducir la superficie de ataque	21,5	**4 semanas** 1 semana diseño + 2 semanas configuración + 1 semana puesta en marcha	**21,5** **Máxima**
MR4. Creación de entornos defendibles	21,5	**4 semanas** 1 semana diseño + 2 semanas configuración + 1 semana puesta en marcha	**21,5** **Máxima**
MR5. Gestión de la autenticación	18,87	**7 semanas** 3 semanas implementar autenticación multi factor + 3 semana reducir privilegios usuarios + 1 semana políticas contraseñas	**4,72** **Media**
MR6. Implementación de acceso remoto seguro	19,75	**8 semanas** 1 semana eliminar accesos traseros + 1 semana aplicar políticas + 1 semana tareas administrativas	**6,58** **Media**
MR7. Monitorización y respuesta	19,43	**4 semanas** 1 semana diseño + 1 semana configuración + 1 semana puesta en marcha + 2 semanas pruebas	**19,43** **Máxima**

[10] RMR se trata del riesgo medio de los escenarios en los que la Medida de Mitigación de Riesgos está implicada
[11] La prioridad se ha calculado como la división entre RMR y su coste temporal

Tabla 40. Priorización y estimación de coste temporal de las medidas de mitigación de riesgos MR8 - MR14.

Medida Mitigación de Riesgos	RMR	Estimación de coste temporal	Prioridad
MR8. Plan de concienciación al personal	13,78	**10 semanas** 5 semanas diseño del programa de concienciación + 5 semanas duración del plan de concienciación	**1,39** **Baja**
MR9. Gestión de las copias de seguridad	10,03	**8 semanas** 4 semanas configuración y 4 semanas puesta en marcha	**5,01** **Media**
MR10. Realizar evaluaciones periódicas de ciberseguridad	25	**8 semana** 4 semanas organización y 4 semanas diseño	**6,25** **Media**
MR11. Desarrollar e implementar una política de seguridad	14,41	**16 semanas** 4 semanas organización y 12 semanas diseño	**0,9** **Muy Baja**
MR12. Mejora en la gestión de incidentes y atención al usuario	14,97	**8 semana** 1 semana organización y 7 semanas diseño	**15,42** **Alta**
MR13. Uso de protocolos de comunicación seguros	25	**12 semanas** Con impacto en producción y alto coste económico	**6,25** **Media**
MR14. Diseño e implantación de un Plan Director de Seguridad Física	17,47	**48 semanas** Fuera del alcance de este proyecto	**0,17** **Muy Baja**

En la Figura 23, se recoge un resumen de la tabla anterior, siendo la barra roja la prioridad de la medida. Se puede observar como las medidas "MR3. Reducir la superficie de ataque", "MR4. Creación de entornos defendibles" y "MR7. Monitorización y respuesta" son las más prioritarias.

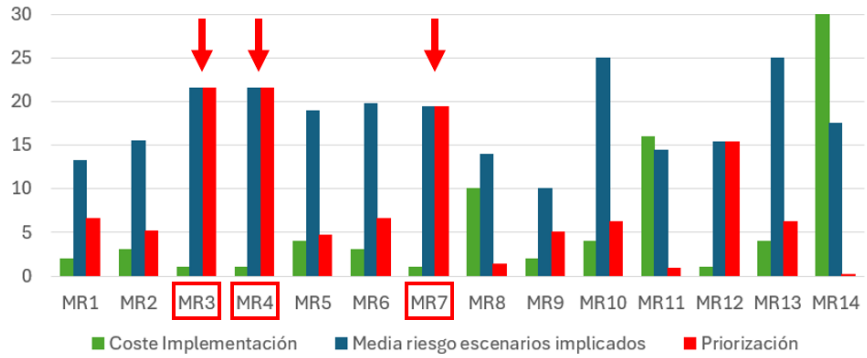

Figura 23. Priorización de las medidas de mitigación de riesgos.

3.5 Aprobar el Plan Director de Seguridad

El plan que se ha definido debe ser revisado y aprobado por la Dirección. Es posible que al revisar el Plan Director de Seguridad (PDS) se deba modificar el alcance, duración o prioridad de los proyectos. El proceso de revisión podría repetirse cíclicamente hasta obtener una versión final que sea aprobada por la Dirección. Una vez se haya obtenido la versión definitiva del Plan Director de Seguridad, se comunicará a todos los empleados de la organización. Es importante que la organización lo entienda y colabore con él.

3.6 Puesta en marcha

Una vez el Plan Director de Seguridad (PDS) haya sido aprobado por la Dirección, se llevará a cabo la metodología de gestión de proyectos que la organización considere más oportuna.

Existen una serie de aspectos que favorecerán que el proyecto sea un éxito:

- Se debe llevar a cabo una presentación general del proyecto a las personas implicadas informándoles de qué trabajos se deben realizar y qué objetivos se persiguen.
- Asignar responsables y coordinadores de proyectos y dotarlos de los recursos que sean necesarios. Dependiendo de la envergadura del proyecto, puede ser necesario formar un Comité de Gestión que se encargue de supervisarlo.
- Establecer la periodicidad con la que se debe realizar el seguimiento del Plan Director de Seguridad.
- Conforme se alcancen los hitos previstos, se debe confirmar que las deficiencias que se hayan identificado en las auditorías o análisis de riesgos se hayan subsanado.

3.7 Análisis del cumplimiento de los requisitos y objetivos del PDS

Tras el análisis de riesgos y la implantación de las medidas de mitigación de riesgos, se verifica el cumplimiento de los objetivos establecidos para cada uno de los Requisitos Fundamentales (FR – Fundamental Requirements) y requisitos individuales del sistema de control (SR), de la norma IEC 62443 [2], para el Plan Director de Ciberseguridad (PDS).

Tabla 41. Análisis del cumplimiento de los requisitos y objetivos FR1.

Requisito del Sistema	Mitigación de Riesgos (MR)														SL -C	SL -T	SL -A
	1	2	3	4	5	6	7	8	9	10	11	12	13	14			
FR 1. Control de identificación y autenticación															2	3	4
SR 1.1. Identificación y autenticación de usuarios humanos					X						X			X			
SR 1.2. Identificación y autenticación de procesos de software					X						X						
SR 1.3. Gestión de cuentas					X						X						
SR 1.4. Gestión de identificadores					X						X						
SR 1.5. Gestión de autenticadores					X						X						
SR 1.6. Gestión de acceso inalámbrico					X						X						
SR 1.7. Fortaleza de la autenticación basada en contraseña					X			X			X						
SR 1.8. Certificados de infraestructura de clave pública (PKI)					X						X						
SR 1.9. Fortaleza de la autenticación de clave pública					X						X						
SR 1.10. Retroalimentación del autenticador					X						X						
SR 1.11. Intentos fallidos de inicio de sesión					X						X						
SR 1.12. Aviso de uso del sistema					X						X						
SR 1.13. Acceso a través de redes que no son de no confianza					X	X		X			X						

Tabla 42. Análisis del cumplimiento de los requisitos y objetivos FR2 – FR6.

Requisito del Sistema	Mitigación de Riesgos (MR)														SL-C	SL-T	SL-A
	1	2	3	4	5	6	7	8	9	10	11	12	13	14			
FR 2. Control de uso															1	2	4
SR 2.1. Aplicación de la autorización					X						X						
SR 2.2. Control de uso inalámbrico					X						X						
SR 2.3. Control de uso para dispositivos portátiles y móviles					X						X						
SR 2.4. Código móvil					X						X						
SR 2.5. Bloqueo de la sesión					X						X						
SR 2.6. Terminar una sesión remota					X	X					X						
SR 2.7. Control de las sesiones simultáneas					X						X						
SR 2.8. Eventos auditables										X	X						
SR 2.9. Capacidad de almacenamiento de datos de auditoría									X		X						
SR 2.10. Respuesta a los fallos de procesamiento de auditorías										X	X						
SR 2.11. Marcas de tiempo							X				X						
SR 2.12. No rechazo											X						
FR 3. Integridad del sistema															2	2	4
SR 3.1. Integridad de la comunicación					X						X		X				
SR 3.2. Protección contra códigos maliciosos		X					X	X			X						
SR 3.3. Verificación de la funcionalidad de la seguridad										X	X						
SR 3.4. Integridad del software y de la información	X	X					X	X			X						
SR 3.5. Validación de entrada							X				X						
SR 3.6. Salida determinista							X				X						
SR 3.7. Tratamiento de errores											X	X					
SR 3.8. Integridad de la sesión					X						X		X				
SR 3.9. Protección contra la información de auditoría					X				X		X						
FR 4. Confidencialidad de los datos															1	2	4
SR 4.1. Confidencialidad de la información								X	X		X						
SR 4.2. Persistenia de la información									X		X						
SR 4.3. Uso de criptografía									X		X						
FR 5. Flujo de datos restringido															2	4	4
SR 5.1. Segmentación de red			X	X							X						
SR 5.2. Protección de los límites de la zona			X	X							X						
SR 5.3. Restricciones de comunicación entre personas de propósito general				X				X			X						
SR 5.4. Partición de aplicaciones	X	X						X			X						
FR 6. Respuesta oportuna a los Incidentes															2	3	4
SR 6.1. Accesibilidad de los registros de auditoría					X						X						
SR 6.2. Supervisión contínua										X	X						

Tabla 43. Análisis del cumplimiento de los requisitos y objetivos FR7 y recuento.

Requisito del Sistema	Mitigación de Riesgos (MR)														SL-C	SL-T	SL-A
FR 7. Disponibilidad de recursos															2	4	4
SR 7.1. Protección contra la denegación de servicio		X				X					X	X		X			
SR 7.2. Gestión de recursos		X									X	X					
SR 7.3. Copia de seguridad del sistema de control									X		X	X					
SR 7.4. Recuperación y reconstrucción del sistema de control									X		X	X					
SR 7.5. Alimentación de emergencia											X	X					
SR 7.6. Ajustes de configuración de red y seguridad											X						
SR 7.7. Funcionalidad mínima											X	X					
SR 7.8. Inventario de componentes del sistema de control								X			X						
Recuento de Requisitos involucrados en los MR	2	5	2	3	24	3	5	8	7	4	51	7	2	2			

Se observa como "MR5. Gestión de la autenticación" y "MR11. Desarrollar e implementar una política de seguridad" son las medidas de mitigación de riesgos que más requisitos de la norma tienen. Esto se debe a que en la norma hay muchos requisitos relacionados con la autenticación, y que desarrollar e implementar una política de seguridad abarca muchos de los requisitos mencionados.

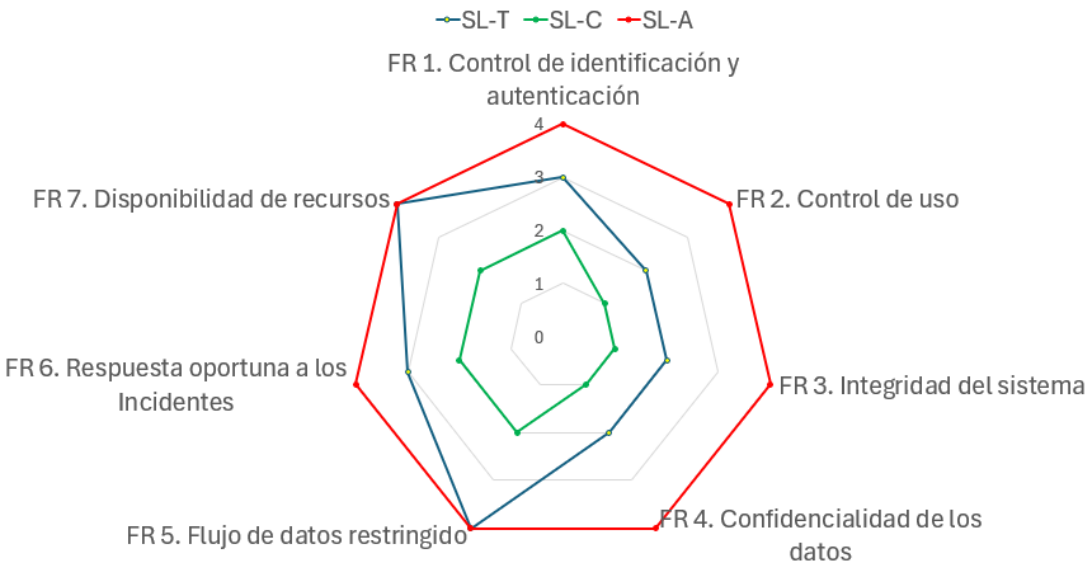

Figura 24. Análisis del cumplimiento de los requisitos y objetivos.

Finalmente, en la Figura 24, se representa de manera gráfica los niveles de seguridad de capacidad (SL-C), objetivo (SL-T) y alcanzado (SL-A).

4 INFRASTRUCTURA DE LA SUBESTACIÓN ELÉCTRICA

El objetivo de las subestaciones eléctricas es modificar el nivel de tensión para poder dedicarlo a distintas aplicaciones como por ejemplo el alumbrado público, residencias o la industria entre otras. Se compone de distintos equipos eléctricos, destinados a la transferencia de energía eléctrica, basándose en la transformación de potencia. Los equipos de subestaciones se encargan de hacer interactuar varios circuitos eléctricos, otorgando funciones de maniobra, protección y supervisión, que permitan el funcionamiento seguro de una subestación [47].

Las subestaciones eléctricas se tratan de infraestructura crítica, que debe ser debidamente protegida, tanto física como cibernéticamente. En los últimos años, con la hiperconectividad que han sufrido todos los entornos, los sistemas de energía eléctrica se han convertido en sistemas de información distribuidos que se comunican haciendo uso de protocolos abiertos [48]. La vida útil de los sistemas de control se estima que es de 20 a 30 años, y cuando se diseñaron de manera aislada, no estaban preparados para ser entornos cibernéticamente seguros.

4.1 Normativa

Las subestaciones eléctricas en España tienen que cumplir una serie de normas de obligado cumplimiento que se recogen en el siguiente documento "Reglamento sobre centrales eléctricas, subestaciones y centros de transformación" [49]. El objetivo de esta normativa es:

1. Proteger las personas y la integridad y funcionalidad de los bienes que pueden resultar afectados por las mismas instalaciones
2. Conseguir la necesaria regularidad en los suministros de energía eléctrica
3. Establecer la normalización precisa para reducir la extensa tipificación que existe en la fabricación de material eléctrico
4. La óptima utilización de las inversiones, para facilitar la posibilidad de adaptar las instalaciones a futuros aumentos de carga

En esta relación de normas, se pueden extraer las algunas de las categorías:

- Ensayos.
- Aislamiento.
- Símbolos literales/gráficos utilizados en electrotecnia.
- Elementos de la subestación: Transformadores, interruptores, seccionadores…
- Protecciones.
- Instalación.

Además, si el Ministerio de Industria y Energía lo estima oportuno puede establecer la homologación de un tipo de máquina o aparato utilizable en las instalaciones.

4.1.1 Normativa específica de ciberseguridad en Subestaciones Eléctricas

Existe normativa específica para las comunicaciones en las subestaciones eléctricas, la norma "IEC 62351 - Gestión de sistemas de potencia e intercambio de información asociada. Seguridad de datos y comunicaciones" [10].

Tal y como se recoge en el artículo "Cybersecurity Based on IEC 62351 and IEC 62443 for IEC 61850 Systems" de "Schweitzer Engineering Laboratories, Inc" [50], la norma IEC 62351 tiene un enfoque de seguridad a nivel de dispositivo y comunicaciones, es decir, requiere de autenticación, uso de canales redundantes o mecanismos de desafío y respuesta [51], mientras que la norma IEC 62443-3, aplica una estrategia de defensa en profundidad para redes OT (Operational Technology – Tecnología Operacional), que permite implementar los controles de seguridad correctos en cada capa del Sistema de Control Industrial sin degradar su rendimiento [50].

Además, no debe dejarse de lado la norma ISO/IEC 27001 [6]. Se trata de un estándar más genérico para gestionar los riesgos de la seguridad de la información [52].

Por lo que, para una adecuada política de seguridad, deberían aplicarse los estándares IEC 62351, IEC 62443 e ISO/IEC 27001 en paralelo. En la Figura 25, se aprecia como se reparte la aplicación de la normativa:

- ISO/IEC 27001 para la infraestructura IT desde el punto de vista del operador de los activos con una perspectiva procedural, esto es, requisitos para el desarrollo del proceso y Sistema de Gestión de Información de Seguridad (ISMS - Information Security Management System) para el operador y fabricantes.
- IEC 62443 para la infraestructura IT desde el punto de vista del integrador y operador de los activos, con un enfoque procedural y funcional, proporcionando niveles de seguridad y robustez de las medidas de seguridad.
- IEC 62351 tiene un enfoque técnico, en cuanto a medidas de seguridad en la implementación y apoyo a la interoperabilidad, desde el punto de vista del proveedor del producto y el integrador.

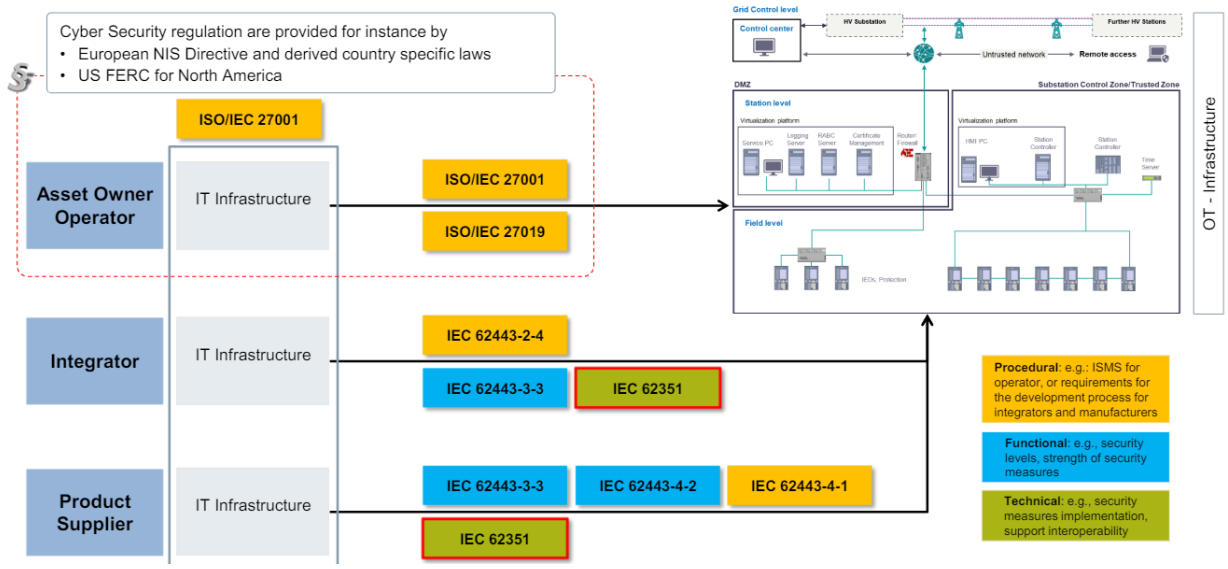

Figura 25. Ciberseguridad para la automatización de sistemas de energía: Interacción de ISO/IEC 27001 / IEC 62443 / IEC 62351 [53].

4.2 Tipos de Subestaciones Eléctricas

A continuación, se pueden observar los diferentes tipos de subestaciones eléctricas, empezando por las centrales generadoras hasta llegar a las subestaciones de distribución de baja tensión.

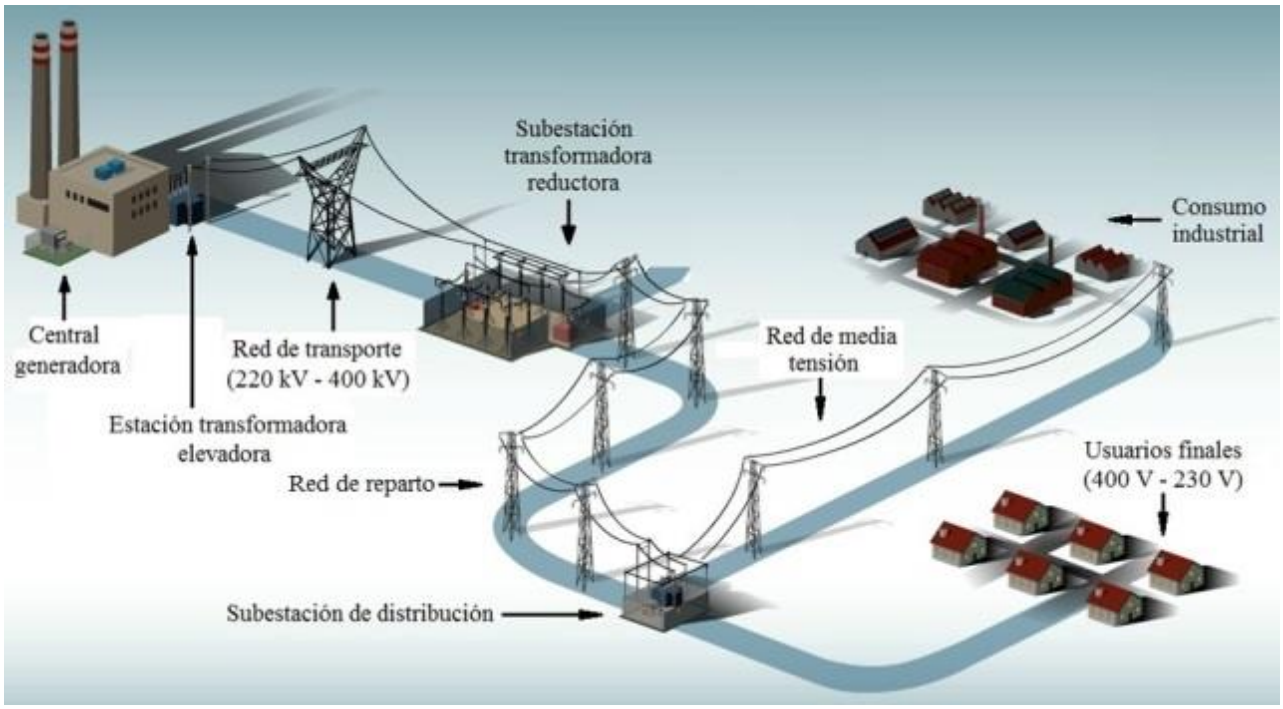

Figura 26. Tipos de Subestaciones Eléctricas [54].

Se presentan algunos detalles de cada uno de los tipos de subestaciones eléctricas mostradas en la Figura 26, a partir de la información de la referencia [55].

- **Las centrales generadoras:** Son aquellas donde se produce la energía eléctrica. Pueden ser centrales eólicas, solares, nucleares, hidráulica o térmica y pueden producir una tensión de entre 3 y 20 kV.
- **Subestaciones elevadoras:** Se sitúan al lado de las centrales de generación para elevar la tensión, reduciendo así la corriente, (ya que la potencia se mantiene constante), permitiendo reducir las pérdidas en el transporte de la energía eléctrica, que son proporcionales al cuadrado de la intensidad.
- **Subestaciones reductoras:** Se ubican próximas a núcleos de gran consumo. Se encargan de reducir la tensión del nivel de transporte (entre 220 kV y 400 kV) hasta un nivel óptimo para el reparto (entre 25 kV y 132 kV).
- **Subestaciones de distribución:** Se transforma la tensión a un nivel más apropiado para distribuir la energía eléctrica (entre 10 y 25 kV).
- **Centros de transformación:** Se encargan de reducir la tensión de la red de distribución hasta baja tensión, desde 230 V en monofásica hasta 400 V en trifásica.

Los consumidores finales reciben la energía eléctrica que procede de la red de distribución. Pueden ser hogares o industrias. El suministro elécrtico de los usuarios finales suele hacerse en alterna monofásica de 230 V, que proviene de conectarse a una de las fases de la red trifásica de 400 V.

4.3 Elementos principales de una subestación

Una subestación eléctrica está formada por distintos circuitos eléctricos que se conectan mediante un sistema de barras conductoras, cada circuito eléctrico está compuesto por interruptores, transformadores, y seccionadores, entre otros dispositivos [56].

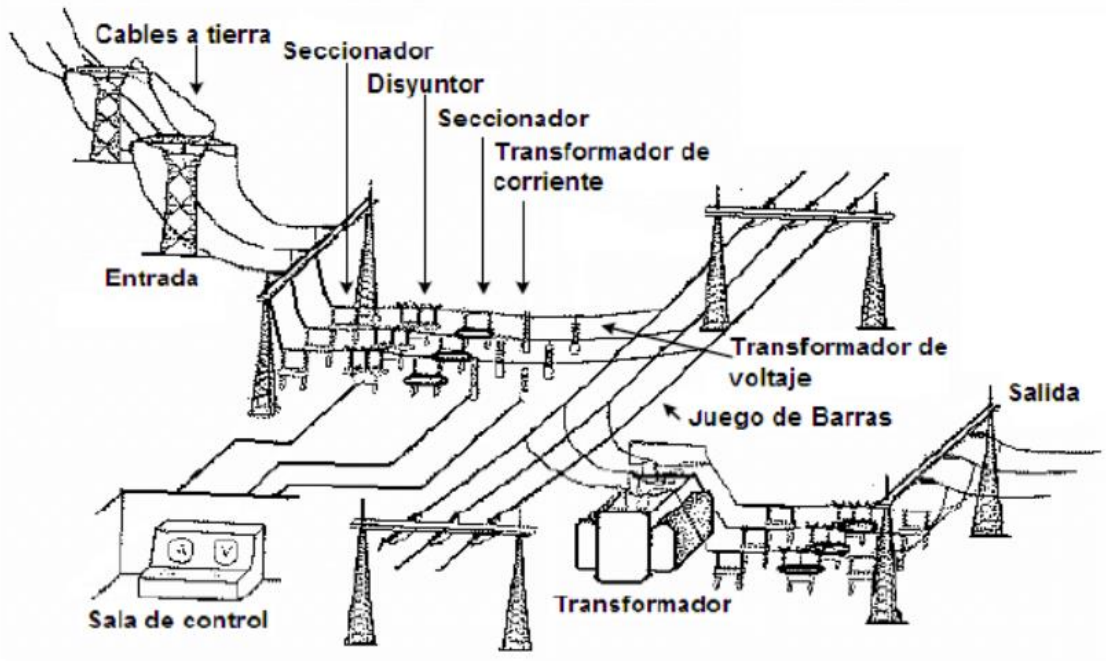

Figura 27. Elementos de una subestación eléctrica [57].

Los elementos de una subestación eléctrica se pueden ver ordenados en la Figura 27. Se describen a continuación:

- **Interruptor**: Este dispositivo se utiliza para la apertura o cierre de los circuitos eléctricos, de igual manera garantizan la protección de estos contra cortocircuitos [47].
- **Transformador**: Es un elemento encargado de elevar o reducir niveles de tensión, mediante relaciones de transformación entre su devanado primario y secundario, bajo el principio de inducción electromagnética, se caracteriza por mantener la frecuencia constante.
    - De voltaje y corriente.
    - De potencia.
- **Disyuntor**: Se encargan de transformar la tensión y aislar los instrumentos de medición y protección conectados a los circuitos de alta tensión.
- **Seccionador**: Se utiliza para aislar eléctricamente una instalación, sirven para brindar seguridad en las labores de mantenimiento.
- **Fusible**: Protege a un circuito eléctrico de sobrecorriente.
- **Pararrayos**: Protege a los equipos eléctricos contra sobrevoltajes de origen atmosférico.
- **Aisladores**: Separan las barras conductoras evitando arcos eléctricos entre las mismas.
- **Relés**: Dispositivos de protección.

4.4 Automatización de Subestaciones Eléctricas

La automatización de subestaciones eléctricas consiste en la integración de los equipos de patio, maniobra y control mediante protocolos de comunicación de manera que se pueda monitorizar de manera local o remota para poder analizar la información y verificar el funcionamiento adecuado de la subestación.

Para ello se implementa un sistema de control y adquisición de datos (SCADA), que aplicado a las subestaciones eléctricas, debe monitorizar y controlar los valores de coltaje, corriente, potencia y los estados de los dispositivos de campo.

4.5 Ciberseguridad en Subestaciones Eléctricas

En el siguiente apartado se revisarán las vulnerabilidades y las consecuencias de un ciberataque sobre una subestación eléctrica.

4.5.1 Vulnerabilidades en las Subestaciones Eléctricas

Siguiendo la norma IEC 62351 [10], se destacan las siguientes brechas de seguridad de los sistemas de control de infraestructuras energéticas.

- **Comunicaciones abiertas:** Se utilizan normas y protocolos de transmisión abiertos y conexiones a redes públicas. Lo que supone una vulnerabilidad crítica.
- **Falta de concienciación sobre la ciberseguridad**: El personal no suele estar formado en términos de ciberseguridad y usan dispositivos conectados a la red de la planta.
- **No se siguen los requisitos de seguridad**: La configuración de los equipos o el diseño de la arquitectura de la red no sigue los requisitos de seguridad.
- **Complejidades de control de acceso:** El control de acceso, tanto físico como virtual, debe llevarse a cabo de manera efectiva, controlando los permisos que tiene cada usuario para acceder a qué recursos.
- **Vida útil prolongada de los componentes**: La vida útil de los componentes de un sistema de control industrial puede ser de entre 20 y 30 años. Por lo que si una planta industrial se diseñó de manera aislada, sin considerar que la planta se conectaría al exterior, no cumplirá con unos requisitos mínimos de seguridad.

Mediante las medidas propuestas en el Plan Director de Ciberseguridad, se logran controlar dichas vulnerabilidades, como se ha estudiado en el apartado “3.1.8 Nivel de riesgo aceptable”.

4.5.2 Consecuencias de un ciberataque a una Subestación Eléctrica

Un ciberataque a una subestación eléctrica puede ser catastrófico, con un impacto principal en la seguridad y salud de la población. Las posibles consecuencias de un ciberataque a una subestación eléctrica son:

- Los hogares se quedarían sin suministro eléctrico, es decir: sin calefacción, sin comunicaciones y sin luz ni cocina eléctrica.
- El transporte público dependiente de la energía eléctrica se detendría, como el metro o el tren.

- En la industria, casi la mitad de la energía que se consume es eléctrica [58]. Por lo que si el corte eléctrico afectara a una planta industrial podría detener su producción y provocar pérdidas económicas muy elevadas a la misma. Incluso si se detuviera una maquinaria o un proceso químico concreto, podría provocar un impacto en la salud de la población, si no se toman las medidas adecuadas.
- Los hospitales quedarían sin suministro eléctrico, pudiendo afectar a operaciones quirúrjicas que estén en curso o incluso a personas que sean dependientes a la electricidad.
- Los medios de comunicación: la radio, la televisión y el acceso a internet, se verían directamente afectados, pudiendo provocar el corte total de las comunicaciones.
- Supondría un escenario desfavorable en caso de conflicto militar.

Un ejemplo de ciberataque dirigido a un sistema eléctrico, diferente a los revisados en el apartado "1.4.2. Actores de amenazas" es el caso de BlackEnergy. En el 2015, el malware BlackEnergy fue utilizado en Ucrania contra medios de comunicación y empresas del sector eléctrico. Los atacantes produjeron un corte en el suministro eléctrico provocando un apagón y lanzaron una denegación de servicio para impedir que llegaran los reportes de los usuarios. Adicionalmente trataron de dañar los sistemas SCADA para dificultar la reactivación del sistema eléctrico.

4.6 Infraestructura de partida de la subestación propuesta

Se toma de partida el proyecto de ejecución de "Diseño e Implementación De Un Sistema SCADA Para Control y Monitoreo De La Subestación Eléctrica San Gabriel" [59], ubicada en Ecuador. Forma parte de un conjunto de subestaciones eléctricas de la Empresa Eléctrica Regional del Norte. El proyecto completo se encuentra en las referencias. En esta sección se detallan los dispositivos de red y la arquitectura del sistema SCADA.

En la Tabla 44, se recogen los elementos de la infraestructura de la Subestación Eléctrica de San Gabriel, el nombre, una descripción y la cantidad de elementos que hay de cada tipo.

Tabla 44. Elementos de la infraestructura de partida.

Nombre	Descripción	Cantidad
Medidor ION 8600	Esclavos modbus que monitorizan la red eléctrica para mandarla al maestro.	5
Medidor ION 6200	Medidor auxiliar	1
PLC S7 1200	Maestro modbus que recopila la información de la red eléctrica.	1
Switch	Encargados de interconectar los distintos elementos de red entre sí.	4
Router	Encargado de enrutar los paquetes dentro de la subestación y actúa como puerta de salida al exterior (gateway).	1

4.6.1 Medidores ION 8600

Los medidores ION 8600 están instalados en los alimentadores y el transformador de 13.8kV de la subestación eléctrica de San Gabriel, el cual, es capaz de recabar medidas precisas de Voltaje, Corriente, Potencia y Energía. Adicionalmente, es capaz de medir la calidad de la energía y comprueba el cumplimiento de las capacidades de entrada y salida. Utiliza diversos protocolos de comunicación, entre ellos, Modbus TCP.

Figura 28. Medidor ION 8600 [56]

Usa el puerto preconfigurado (502), y se comunica mediante el puerto Ethernet integrado, este puede ser configurado ya sea como maestro o como esclavo, cuando actúa como maestro Modbus puede escribir datos y leer datos de dispositivos esclavos Modbus, de similar forma cuando se configura como esclavo, se puede acceder a los datos del medidor desde algún dispositivo maestro.

Tabla 45. Direccionamiento de las Variables del Medidor

Dirección Modbus	Descripción
40150	Ia
40151	Ib
40152	Ic
40163	V umbral
40164	I umbral
40178 a 40179	Vab
40180 a 40181	Vbc
40182 a 40183	Vca
40166 a 40167	Va
40168 a 40169	Vb
40170 a 40171	Vc

Dirección Modbus	Descripción
40204 a 40205	kW tot
40214 a 40215	Kvar tot
40230 a 40231	kWh del
40232 a 40233	kWh rec
40234 a 40235	kVARhdel
40236 a 40237	kVARhrec
40238 a 40181	kVARh del + rec
40182 a 40239	FP
40265	THD V
40268	THD I

4.6.2 PLC S7 1200

En este caso el PLC S7 1200 va a actuar como Maestro y cada medidor será un Esclavo. Mediante la tabla proporcionada, en la base de datos del PLC S7 1200, deberá acceder a las direcciones que se han especificado para obtener los datos requeridos.

Figura 29. PLC S7 1200 [56]

4.6.3 Arquitectura de red de comunicaciones

La arquitectura de red de comunicaciones de partida es la siguiente:

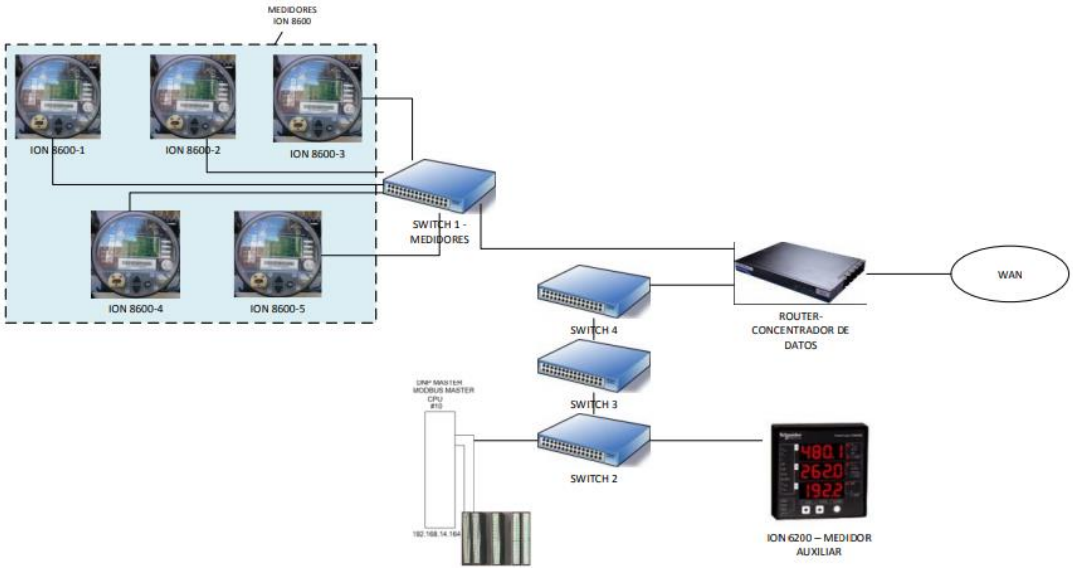

Figura 30. Diagrama de comunicaciones del sistema SCADA de la Subestación Eléctrica [56]

Se toman los dispositivos y la arquitectura de red de partida para tomar las medidas que se consideren oportunas en el Plan Director de Seguridad para poder mitigar los riesgos de la misma. Por ejemplo, como se verá más adelante, se planteará:

- Reducir la superficie de ataque, aislando la red del Sistema de Control Industrial (ICS) de cualquier otra red no confiable
- Segmentar la red en enclaves lógicos, para crear un entorno defendible.
- Monitorizar la red para detectar software malicioso e intentos de ataque

4.6.4 Protocolo Modbus TCP

Se trata de un protocolo de comunicaciones altamente extendido en Sistemas de Control Industrial (ICS) debido a que es ligero y simple. Se basa en la arquitectura maestro/esclavo, donde el maestro se encarga de enviar ordenes a uno o más esclavos, mientras que ellos se encargan de responder a las peticiones que realiza el maestro.

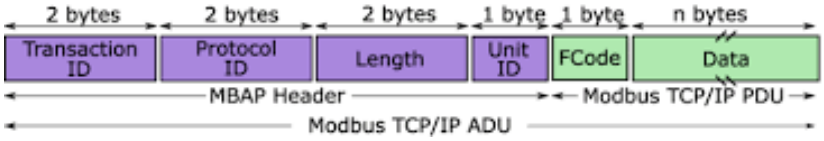

Figura 31. Modbus TCP ADU (Application Data Unit – Unidad de Datos de Aplicación) [60]

En la Figura 31, se muestra un paquete Modbus TCP/IP ADU, que incluyen una cabecera MBAP (MODBUS Application Protocol Header – Cabecera de Aplicación de MODBUS) y una PDU (Protocol Data Unit – Unidad de Datos de Protocolo) con los siguientes campos:

- Transaction ID: Es el identificador de petición Maestro/Esclavo.
- Protocol ID: Es el identificador de protocolo, en el caso de Modbus TCP es “00 00”.
- Longitud: Es el número de bytes que tiene el mensaje Modbus.
- Unit ID: Es el identificador de la instancia de Modbus en el equipo destinatario.
- Function Code: Es un código que identifica la función Modbus. El campo es de 1 byte, pero existen códigos de función desde el 0 hasta el 127, para que el bit más significativo siempre sea 0. En el caso de que el bit más significativo sea 1, indica que se ha producido una excepción.
- Datos: Depende de la función empleada el contenido varía.

El tamaño de PDU de Modbus tiene un máximo de 253 bytes, añadiendo los 7 bytes de la cabecera MBAP, formando un total de 260 bytes máximos. Existen tres tipos de PDU: petición, respuesta o excepción.

El modelo de datos que sigue Modbus consta de:

- Objetos de 1 bit (Coils ó Discrete Inputs)
- Objetos de 16 bits (Holding Registers o Input Registers)

Los objetos de tipo Coil o Holding Register son modificados y leídos por aplicaciones que utilizan el protocolo Modbus, mientras que los Discrete Inputs y Input Registers son objetos de sólo lectura por sistemas I/O.

El protocolo Modbus cuenta con funciones que permiten a un Maestro realizar acciones sobre los dispositivos Esclavos. Existen tres categorías de funciones:

- Funciones públicas: Se trata de funciones estándar y apoyadas por la comunidad modbus.org.
- Funciones definidas por el usuario: Permite que los usuarios definan sus funciones, cuyos rangos se encuentran entre 65-72 (0x41 a 0x58) y 100-110 (0x64 a 0x6E).
- Funciones reservadas: Utilizadas por algunas empresas para productos específicos, y no son funciones públicas. Por ejemplo, la función 90 (0x5A) usada por Schneider Electric para subir o descargar código de programación de un PLC.

En la Tabla 46, se pueden observar las funciones públicas que resultan de más interés para este trabajo junto con sus códigos de función en formato decimal.

Tabla 46. Funciones Modbus relevantes para el trabajo

Código	Nombre	Tipo	Sub-función
01	Read Coils	Acceso de datos (1-Bit)	-
03	Read Holding Registers	Acceso de datos (16-Bits)	-
04	Read Input Registers	Acceso de datos (16-Bits)	-
05	Write Single Coil	Acceso de datos (16-Bits)	-
06	Write Single Register	Acceso de datos (16-Bits)	-
15	Write Multiple Coils	Acceso de datos (16-Bits)	-
16	Write Multiple Registers	Acceso de datos (16-Bits)	-
17	Report Slave ID	Diagnóstico	-
43	Read Devide Identification	Encapsulated Interface	14. Return Slave Message Count

Se puede ver el total de las funciones Modbus consultando en la referencia [61].

5 MEDIDAS DE MITIGACIÓN DE RIESGOS

Se han propuesto catorce medidas de mitigación de riesgos, y se han clasificado en función del impacto y probabilidad de ocurrencia de los riesgos que pretenden mitigar. En la Tabla 47, se presentan las tres medidas más prioritarias para su posterior estudio en los apartados de la memoria recogidos en la tabla.

Tabla 47. Organización de las medidas de mitigación de riesgos en la memoria.

Medida de Mitigación de Riesgos	Media Riesgo Escenarios Implicados (RMR)	Coste temporal	Prioridad	Apartado en la memoria
MR3. Reducir la superficie de ataque	21,5	4	**5,38 Máxima**	5.1 Arquitectura de red propuesta
MR4. Creación de entornos defendibles	21,5	4	**5,38 Máxima**	
MR7. Monitorización y respuesta	19,43	4	**4,86 Máxima**	5.2 Sistema de Detección de Intrusiones (IDS) 5.3 Sistema Gestor de Información y Eventos de Seguridad (SIEM)

A continuación, se analizarán las medidas prioritarias propuestas, para mitigar los riesgos implicados en la infraestructura de la subestación eléctrica mostrada en el apartado anterior.

- **5.1 Arquitectura de red propuesta**

En este apartado se propone una nueva arquitectura de red más segura, debido a que separa la red empresarial (IT) de la red operacional (OT) mediante un tipo de arquitectura de red llamada DMZ (zona desmilitarizada ó red perimetral).

- **5.2 Sistema de Detección de Intrusiones (IDS)**

Se estudian los Sistemas de Detección de Intrusiones para entornos industriales disponibles en el mercado, para proponer el más idóneo para el caso de estudio.

- **5.3 Sistema Gestor de Información y Eventos de Seguridad (SIEM)**

Se estudian los Sistemas Gestores de Información y Eventos de Seguridad para entornos industriales disponibles en el mercado, para proponer el más idóneo para el caso de estudio.

5.1 Arquitectura de red propuesta

En este apartado se pretende diseñar la red del entorno industrial en cuestión, pretendiendo ser lo más fiel posible a un entorno de producción real. Este apartado engloba las medidas de mitigación de riesgos "MR3. Reducir la superficie de ataque" y "MR4. Creación de entornos defendibles".

5.1.1 Segmentación física de la red

En primer lugar se identifican los conductos que comunican las distintas zonas, identificadas en el apartado "5.1.1 Identificación del sistema en consideración". El diseño de la arquitectura de red, está basado en el modelo de Purdue, recogido en la norma IEC 62443-3 [2], el cual segmenta la red en 6 niveles, separando la red empresarial (IT) de la red de operación (OT). En la red empresarial se encuentran los servidores web, de correo, servidor DNS (Domain Name System – Sistema de Nombres de Dominio) y las estaciones de trabajo empresariales. En la DMZ (Demilitarized Zone – Zona Desmilitarizada) se encuentra el Servidor de parches, la copia de seguridad del Historian (donde se almacenan logs e informes de los datos históricos de la planta), un servidor de salto, el SOC (Security Operations Center - Centro de Operaciones de Seguridad) y el SIEM (Security Information and Event Management - Gestor de eventos e información de seguridad). En la red OT se sitúan las estaciones de trabajo de los operadores de la planta, el Historian, el sensor IDS, el HMI (Human Machine Interface – Interfaz Hombre Máquina) y MTU del sistema SCADA, el servidor de salto remoto y los equipos de campo (PLC, RTU, Sensores y Actuadores).

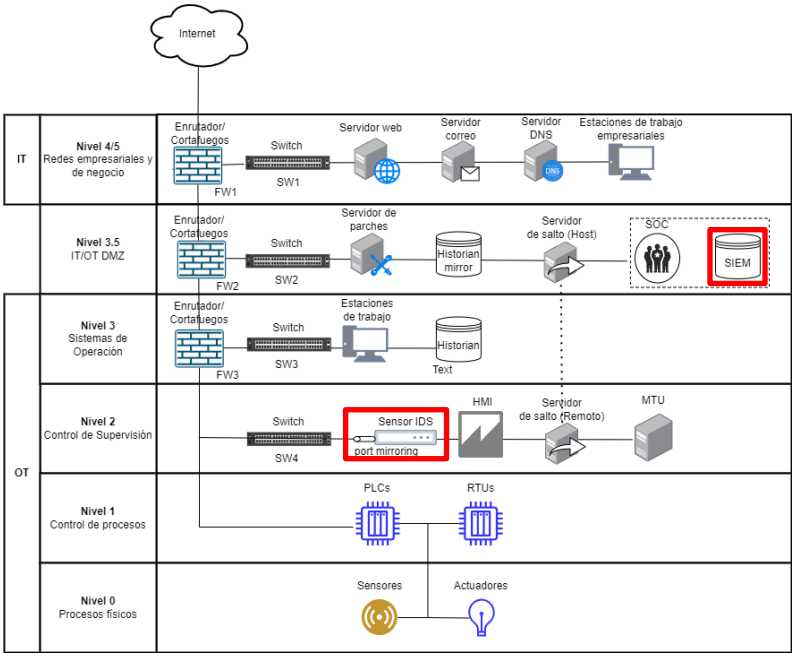

Figura 32. Arquitectura propuesta.

Se puede observar en la Figura 32, como en aquellos conductos (puntos de acceso entre zonas) que conectan los niveles 4/5, 3.5 y 3, se ha configurado un firewall, formando la DMZ. Además, el sensor IDS se encontraría ubicado en el Nivel 2 del modelo, y el SIEM en el Nivel 3.5 [62].

Se ha situado un sensor IDS que se encargue de monitorizar los niveles de procesos físicos, control de procesos y control de supervisión, en la parte OT, mediante un "port mirroring" del switch de esta misma zona, es decir, el switch replicará por el puerto que está conectado al sensor IDS el tráfico que pasa por el resto de los puertos, permitiendo así al sensor IDS capturarlo y analizarlo.

Para situar los elementos de la arquitectura de partida propuesta en el apartado "4.6.3 Arquitectura de red de comunicaciones", los medidores ION 8600 se encontrarían situados en el nivel 0 de procesos físicos, en el lugar de los sensores y el PLC S7 1200, se encontraría en el nivel 1 de control de procesos, en el lugar de los PLCs.

5.1.2 Segmentación virtual de la red

Para separar las distintas subredes se desglosan las VLAN que se definen en la siguiente tabla. Se han decidido repartir los distintos identificadores de VLAN según la segmentación de red física.

Tabla 48. Segmentación virtual de la red.

ID	Nombre	VLAN-ID	Red	Máscara	Rango	Hosts
6	Enlace FW2-FW3	60	10.60.0.0	255.255.255.252	10.60.0.0 - 10.60.0.3	2
5-4	Red empresarial y de negocio	50	10.40.0.0	255.255.255.240	10.40.0.0 - 10.40.0.15	14
3.5	Zona de Desmilitarización (DMZ)	35	10.35.0.0	255.255.255.248	10.35.0.0 - 10.0.35.0.7	6
3	Sistemas de Operación	30	10.30.0.0	255.255.255.248	10.30.0.0 - 10.0.30.0.7	6
2	Red OT	20	10.20.0.0	255.255.255.240	10.20.0.0-10.20.0.15	14
1	Enlace FW1-FW2	10	10.10.0.0	255.255.255.252	10.10.0.0 - 10.10.0.3	2

- **Red empresarial y de negocio**

Se esperan tener 3 servidores (correo, web y DNS), sumando las 2 direcciones para los enrutadores, 1 SIEM y un grupo de analistas de seguridad para el Centro de Operaciones de Seguridad (SOC) de 2 hosts, y un grupo de estaciones de trabajo empresariales de 2 hosts, se añaden 4 direcciones más de reserva, quedandonos un total de 14 hosts.

- **Zona de Desmilitarización (DMZ)**

Se espera 1 servidor de parches de seguridad, 1 mirror del Historian, 1 servidor de salto a la zona de control y supervisión, 1 dirección para el router y 2 de reserva. En total 6 hosts.

- **Sistemas de Operación**

Se estima un grupo de operadores con 2 estaciones de trabajo de la central, 1 Historian, 1 dirección para el router y 2 direcciones de reserva. Formando un total de 6 hosts.

- **Red OT**

Tomando la subestación eléctrica propuesta, se tienen 8 relés y una dirección para el router, se toma máscara /28 ya que es el menor número que cumple con esta premisa, quedándonos con 5 direcciones de reserva. Serían 9 hosts en total.

5.1.3 Conclusión de la arquitectura propuesta

El modelo de Purdue propuesto en la norma IEC 62443 [2], logra una securización de la red en profundidad, segmentando la red para evitar la comunicación directa de la red empresarial (IT) con la red operacional (OT). Con la arquitectura presentada se cumple con los requisitos que se piden en la norma IEC 62443-3-2, consiguiendo superar los riesgos evaluados en este apartado.

5.2 Sistemas de detección de intrusiones (IDS)

Se trata de uno de los apartados de la medida de mitigación de riesgos "MR7. Monitorización y respuesta". Para dar respuesta a las vulnerabilidades existentes en las redes OT, se han desarrollado arquitecturas, técnicas y sistemas que detectan y previenen accesos no deseados. Los Sistemas de Detección de Intrusiones (IDS), son encargados de detectar usos indebidos y anomalías. Estos sistemas, en sus inicios, fueron pensados para el mundo IT, pero las nuevas necesidades de las redes OT, hacen que se hayan adaptado, examinando adecuadamente los protocolos y mensajes que se envían a través de la red [62].

5.2.1 Diferencias entre Sistemas de Detección de Intrusiones y Sistemas de Prevención de Intrusiones

Los Sistemas de Detección de Intrusiones (IDS – Intrusion Detection System) y los sistemas de prevención de intrusiones (IPS – Intrusion Prevention System) son componentes esenciales en la ciberseguridad de redes y sistemas. Aunque ambos tienen como objetivo proteger contra amenazas cibernéticas, existen diferencias clave en su enfoque y funcionamiento:

- La función principal de un IDS es detectar actividades y comportamientos anómalos o maliciosos en una red o sistema. Cuando un IDS identifica una posible intrusión, genera alertas o notificaciones para que los administradores tomen medidas. Sin embargo, no realiza ninguna acción directa para bloquear o prevenir la intrusión.
- Por otro lado, los IPS (Intrusion Prevention System – Sistema de Prevención de Intrusiones), no solo detectan intrusiones, sino que también toman medidas activas para prevenir o bloquear los ataques detectados. Esto puede incluir la modificación de reglas de firewall, la desconexión de conexiones sospechosas o incluso la reconfiguración de la red para evitar la intrusión.

En IACS, la prioridad suele ser la disponibilidad y la integridad de los sistemas. Aunque la seguridad es fundamental, la implementación de sistemas de prevención de intrusiones (IPS) puede plantear desafíos significativos y riesgos potenciales:

- **Impacto en la Disponibilidad**: Los IPS, al tomar medidas para bloquear el tráfico sospechoso, pueden afectar la disponibilidad de sistemas críticos. En un entorno industrial, la interrupción de servicios eléctricos o procesos es inaceptable y podría tener graves consecuencias, no solo económicas.
- **Riesgo de Falsos Positivos y Falsos Negativos:** Los IPS pueden generar falsos positivos o falsos negativos, lo que puede llevar a la interrupción innecesaria de operaciones o a la falta de detección de amenazas reales, respectivamente.
- **Configuración Compleja:** Configurar adecuadamente un IPS en un entorno industrial complejo puede ser un desafío. Las reglas de bloqueo incorrectas o mal configuradas pueden tener consecuencias catastróficas.
- **Escenarios de Ataque Específicos**: Los entornos industriales tienen sus propios escenarios de ataque y necesidades de seguridad. Los IPS genéricos pueden no ser adecuados para abordar estas amenazas específicas.

En lugar de utilizar IPS, en entornos industriales se prefiere emplear IDS, que permiten la detección temprana de amenazas sin afectar la disponibilidad de los sistemas críticos. Esto brinda a los administradores de seguridad la oportunidad de investigar y responder adecuadamente a las amenazas sin arriesgar la operatividad de la infraestructura industrial.

5.2.2 Clasificación de IDS/IPS

Existen diferencias entre los distintos IDS según su ubicación, métodos y capacidades. En este apartado se clasificarán los distintos tipos de IDS y de IPS.

5.2.2.1 Clasificación de IDS: NIDS y HIDS

Los HIDS se encargan de monitorizar el tráfico de la red en la que se encuentran los dispositivos. Para llevarlo acabo se puede utilizar un TAP (dispositivo que repite la comunicación que se introduce en uno de sus puertos por otro) ó realizar un port mirroring de un switch (replicar el tráfico de sus puertos por otro en el que se conecte el NIDS). Los NIDS monitorizan un host en concreto, por ejemplo, en las redes OT, podrían instalarse en un SCADA.

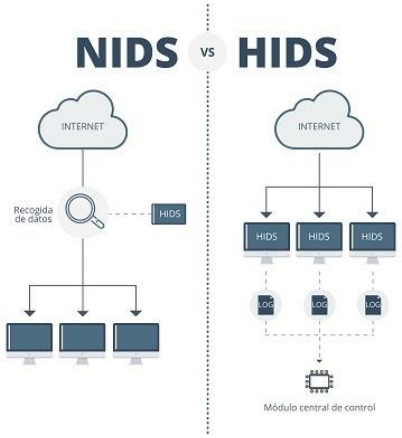

Figura 33. NIDS vs HIDS [63].

5.2.2.2 Clasificación de IPS: EDR, NDR, XDR, MDR y SOAR

Existen distintos tipos de IPS en función de sus capacidades de detección y gestión de incidentes:

- **EDR**: son las sigles del inglés Endpoint Detection and Response, que se traduciría como Detección y respuesta en puntos terminales. Se centran en monitorizar la actividad de los dispositivos terminales (portátiles, ordenadores, servidores…) para detectar comportamientos maliciosos.
- **NDR**: proviene de Network Detection and Response. Se encargan de monitorizar el tráfico de red para detectar posibles amenazas.
- **XDR**: cuyas siglas provienen de Extended Detection and Response, se trata de Detección y respuesta ampliadas. Esta solución se encarga de la correlación de datos de múltiples fuentes (EDR, recursos en la nube…) y de múltiples capas de la infraestructura, por lo que puede descubrir tácticas más sofisticadas que podrían pasar desapercibidas por los EDR convencionales. Suelen integrar análisis avanzados y algoritmos de aprendizaje automático para identificar patrones y anomalías.
- **MDR**: son las siglas en inglés de Detección y Respuesta Gestionada. Es un equipo de seguridad externalizado, se parece mucho a un Centro de Operaciones de Seguridad (SOC) como servicio.
- **SOAR**: proviene de Security Orchestration, Automation, and Response, que se traduciría por Orquestación, automatización y respuesta de seguridad. Su objetivo principal es agilizar las operaciones de seguridad y mejorar la eficacia de la respuesta a incidentes. Mediante el uso de playbooks y la automatización, los equipos de seguridad pueden automatizar las tareas repetitivas, acelerar los tiempos de respuesta y reducir los errores humanos. Permiten realizar un seguimiento y documentar el ciclo de vida de la respuesta a incidentes.

5.2.3 Comparativa de IDS/IPS

Existen numerosos IDS e IPS tanto comerciales como de código abierto. Algunos de ellos son específicos para redes OT, y otros son genéricos, pero se pueden llegar a implementar reglas y decodificadores para detectar protocolos industriales. A continuación, se recopilan los más relevantes, recogiendo en la siguiente tabla sus características principales.

Tabla 49. Comparativa IDS/IPS [12].

Nombre	Entidad	IDS/ IPS	HIDS/ NIDS	EDR/NDR/ XDR/SOAR	opensource /comercial	Integración SIEM
SCADA guardian	Nozomi	IPS	NIDS [64]	XDR	Comercial	Propio, QRadar [65]
GLORIA ICS	CCN Cert	IPS	HIDS [66]	XDR	Comercial	Propio
OSSEC	Atomicorp	IPS	HIDS	XDR	Opensource y Comercial	Wazuh (fork), Atomic OSSEC
Suricata	OISF	IDS	NIDS	-	Opensource	-
Cortex XSOAR	Paloalto networks	IPS	HIDS	SOAR	Comercial	Propio
Falcon	Crowdstrike	IPS	HIDS	EDR	Comercial	Propio
Snort	Snort	IPS	NIDS	EDR	Opensource	Snorby, Elastic Stack
QRadar	IBM	IPS	NIDS	EDR, XDR, MDR y SOAR	Comercial	Propio

Todos ellos tienen en común que utilizan detección basada en firmas y anomalías. Aunque evidentemente, la eficacia de cada uno de ellos dependerá de cómo se hayan configurado, y de si han sido específicamente diseñados para un escenario concreto o no. Además, como se puede observar en la Tabla 49, la mayoría pueden llegar a implementar prevención de intrusiones.

[12] Aquellos que tienen capacidades tanto de IDS como IPS se han subclasificado tanto en HIDS/NIDS como en EDR/NDR/XDR/SOAR.

La Tabla 50, recoge los protocolos de IACS que soportan aquellos de los que se dispone de información disponible en la web:

Tabla 50. Protocolos implementados por los distintos IDS/IPS.

	EtherNet IP	Profinet	EtherCAT	EPL	Modbus TCP	IEC 60870-5-104	DNP3	BACnet	CIP	ControlNet	Profibus	OPC	S7	MQTT
SCADA guardian [67]	X	X	X		X	X	X	X	X			X	X	X
OSSEC [32]						X								
Suricata [68]	X		X		X		X							X
Cortex XSoar [69]	X				X			X					X	
Snort [70]	X				X		X	X	X				X	
QRadar [71]					X	X	X							

La X indica que sí lo implementa. Si no está marcado, no significa que no se pueda llegar a implementar, creando reglas y decodificadores específicos, pero o no lo detecta por defecto o no se ha encontrado ningún artículo al respecto.

5.2.4 Requisitos del IDS para la solución

Los requisitos principales que se deben considerar a la hora de elegir un IDS (IDSR) son:

- **IDSR 1**. Coste de adquisición, mantenimiento y operación del IDS.

Los IDS suponen un coste elevado, tanto de adquisición, como de mantenimiento y operación. Por ello es conveniente elegir un IDS que se ajuste al presupuesto del proyecto.

- **IDSR 2**. Alta capacidad de detección para el protocolo utilizado en la red.

Como el protocolo que utilizan los dispositivos en el escenario industrial seleccionado es Modbus TCP, se pretende que el IDS en cuestión tenga una capacidad de:

  - Identificar qué funciones Modbus se están usando
  - Detectar tamaños ilegales de paquetes
  - Detectar excepciones Modbus

5.2.5 Elección de un IDS para la solución

Para este escenario académico se va a seleccionar Snort [70] como IDS, debido a que es de los que más decodificadores y reglas de protocolos implementa para Modbus TCP. Además, al ser opensource tiene gran variedad de implementaciones con diversos SIEM (Security Information and Event Management - Gestor de eventos e información de seguridad) y herramientas. Y al ser gratuito, se cumple el requisito IDSR 1.

En el trabajo de la referencia [72], titulado "Análisis de la capacidad de detección de Snort sobre ataques de red en ICS bajo la matriz MITRE ATT&CK", se hace un análisis exhaustivo de la capacidad de detección de Snort usando distintos conjuntos de reglas, en diversos protocolos de comunicaciones industriales, como: Modbus TCP, SNP3, S7Comm, CIP, PCCC, SNMP, HTTP y APEX.

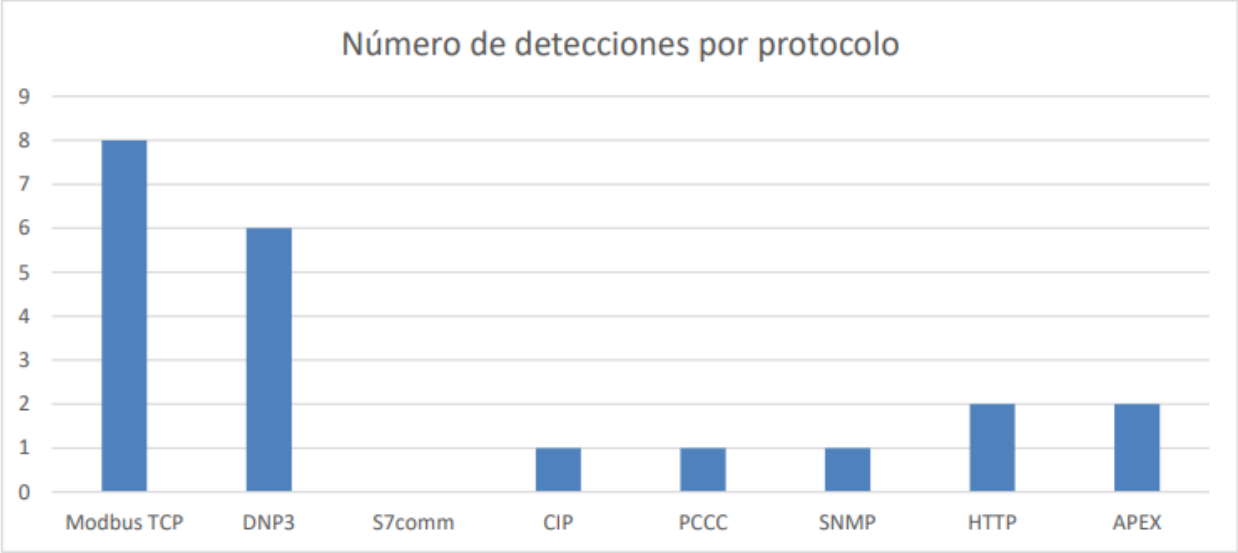

Figura 34. Distribución de las detecciones por protocolo de snort [72].

Para los ataques de Modbus se identificarían qué funciones se están usando, además de detecciones sobre tamaños ilegales de paquetes y excepciones [72], cumpliendo así con el requisito IDSR 2.

5.3 Sistemas Gestores de Eventos de Seguridad (SIEM)

Se trata del último de los apartados de la medida de mitigación de riesgos "MR7. Monitorización y respuesta". Un sistema SIEM o Sistema de Gestión de Eventos e Información de Seguridad, es una herramienta que se utiliza para almacenar e interpretar los datos relevantes de seguridad. Es la herramienta principal utilizada por los operadores de seguridad en un SOC (Security Operations Center – Centro de Operaciones de Seguridad), para poder detectar y responder a incidentes.

Los operadores, se encargarán de recibir alertas de posibles intrusiones, vulnerabilidades o anomalías, y deberán responder en consecuencia, y cumplimentar adecuadamente un informe para tener documentado el suceso. Las principales capacidades de un SIEM son los siguientes, tomados de la referencia [73]:

- **Agregación de datos**: Se refiere a la capacidad de gestionar información proveniente de diversas fuentes.
- **Correlación:** Implica procesar los datos recibidos para convertirlos en información relevante.
- **Alerta:** Consiste en analizar eventos correlacionados para generar notificaciones de seguridad que se envían a un administrador.
- **Cuadros de mando:** Un Sistema de Gestión de Información y Eventos de Seguridad (SIEM) cuenta con herramientas para transformar la información en tablas y gráficos.
- **Cumplimiento:** Gracias a un SIEM, es posible automatizar la recopilación de datos necesarios para elaborar informes sobre normativas existentes.
- **Retención:** Un SIEM tiene la capacidad de almacenar datos a largo plazo, lo cual es fundamental para funciones de análisis forense.
- **Redundancia:** La base de datos de un SIEM suele estar duplicada para evitar la pérdida de datos.
- **Escalabilidad:** Para adaptarse a las necesidades cambiantes en cualquier momento, un SIEM puede configurarse jerárquicamente.

Un sistema SIEM aporta una serie de ventajas a nivel de seguridad: detección temprana de incidentes, análisis forense, centralización de la información, ahorro de recursos e identificación de anomalías.

Figura 35. Arquitectura básica de un SIEM [74].

5.3.1 Particularidades de SIEM en entornos OT

En el contexto de las redes de Tecnología Operativa (OT – Operational Technology), la implementación de un Sistema de Gestión de Información y Eventos de Seguridad (SIEM) no es una tarea sencilla y requiere superar desafíos inherentes a estos entornos [73]:

- **Ciclos de vida prolongados de los dispositivos**: En los entornos industriales, es común que los equipos tengan ciclos de vida muy extensos, llegando incluso a los 40 años según la industria. Esta longevidad plantea retos al desplegar un SIEM, ya que debe adaptarse a tecnologías más antiguas.
- **Limitadas prestaciones de los dispositivos**: Los dispositivos industriales suelen tener capacidades reducidas, diseñadas específicamente para sus tareas. En muchos casos, carecen de la capacidad para generar y enviar registros de eventos (logs). Esto dificulta la generación de eventos de seguridad en un SIEM en entornos de Control Industrial (SCI).
- **Requisitos de conocimientos y habilidad**es: Para utilizar un SIEM de manera efectiva y comprender correctamente los eventos que genera, el personal encargado debe poseer conocimientos específicos del entorno. Esto incluye comprender los protocolos industriales utilizados en el proceso y conocer los equipos industriales.
- **Consideraciones previas al despliegue**: Al implementar un SIEM en entornos industriales, es crucial realizar un análisis exhaustivo de los equipos, las comunicaciones y la topología de red. Esto garantiza una comprensión completa del impacto del SIEM en la red. Además, se debe identificar y priorizar los activos más críticos para el proceso, integrando primero los eventos generados por estos equipos en el SIEM.

El despliegue exitoso de un SIEM en entornos industriales, requiere una planificación cuidadosa y una comprensión profunda de las particularidades de estos sistemas. Esto permitirá que el SIEM aporte valor en términos de ciberseguridad y detecte amenazas en la red donde está implementado. Además, existen grandes diferencias respecto a un SOC para redes IT, tal y como se comentó en la introducción en el apartado "1.2 Incidentes de ciberseguridad industrial".

5.3.2 Comparativa de SIEM

A continuación, se recogen las características de los SIEM más relevantes actualmente, algunos de ellos se corresponden a los que vienen integrados con los IPS que se han visto en el apartado "5.2.3 Comparativa de IDS/IPS".

En la Tabla 51 se recogen SIEMs específicos para OT, y otros genéricos que se han clasificado como IT, pero que también se podrían usar para ICS siempre que se configuren adecuadamente. La mayoría de ellos son comerciales, hay algunos opensource, como Elastic Stack, SIEMonster SMB o AlienValut, pero ofrecen una capa de pago con algunas mejoras y servicio técnico.

Se han clasificado también en función del tipo de despliegue que ofrecen, es decir, si se puede desplegar de manera local en una infraestructura privada, o si se debe usar el despliegue proporcionado por el fabricante en la nube (cloud).

Adicionalmente se refleja en la tabla si el SIEM tiene capacidad de Análisis, Detección o Respuesta. La mayoría de los SIEM no solo permiten almacenar la información de seguridad, también permiten correlarla, para hacer un análisis en profundidad, e incluso responder al incidente.

Tabla 51. Comparativa SIEM.

SIEM	Organización	Tipo	Despliegue	Análisis, Detección, Respuesta	IT/OT	Tamaño organización [13]	Precio [14]
FortiSIEM	Fortinet	Comercial (15 dias prueba)	Cloud o Local	A, D, R	IT y OT [75]	M, L	Muy caro [76]
Sentinel	Microsoft	Comercial (31 dias prueba)	Cloud	A, D	IT	L	Caro [77]
SCADA guardian	Nozomi	Comercial	Local	A, D, R	OT	M, L	Caro [78]
GLORIA ICS	CCN-cert	Comercial	Cloud	A, D	OT	M	Medio
Wazuh	Wazuh	Open source + Comercial	Cloud o Local	A, D	IT	S, M	Bajo
Splunk	Splunk	Comercial (14 dias prueba)	Cloud o Local	A, D	IT y OT	M, L	Medio
Elastic Stack	Elastic	Gratuito + Comercial	Cloud o Local	A	IT	S, M, L	Bajo
Cortex XSOAR	Paloalto networks	Comercial (30 dias prueba)	Cloud o Local	A, D, R	IT y OT	M, L	Medio
QRadar	IBM	Comercial (7 dias prueba)	Cloud o Local	A, D, R	IT	L	Caro
SIEMonster SMB	SIEMonster	Open source + soporte	Local	A	IT	M	Muy bajo
AlienVault	AT&T	Open source + Comercial	Local	A, D	IT	S, M	Muy bajo

[13] Tamaño de la organización: Escala de 3 valores. S (Small): Pequeña, M (Medium): Mediana, L (Large): Grande
[14] Precio: Escala de 5 valores. Muy caro, Caro, Medio, Bajo, Muy bajo

Algunos de los SIEM, requieren de la inversión inicial puesto que se debe utilizar en conjunto con los servidores de monitorización, que se instalan como un dispositivo más en la red para analizar el tráfico. No se está incluyendo el coste de la infraestructura necesaria extra, ya sea un servidor para desplegar el SIEM, firewalls, switches, routers... Esto se verá más en detalle en el apartado de implementación del escenario. Además, el coste anual depende evidentemente de el paquete que se contrate, por lo que se ha tomado un valor estándar para el escenario que se quiere simular en el apartado correspondiente de este trabajo. Algunos se han obtenido a través de las siguientes referencias [79] y [80], pero en general, es necesario contactar con ventas y pasar por un proceso para que evalúen el caso concreto y estimar un precio.

El rango de precios en la tabla anterior oscila desde los 4.000€ hasta los 1.600.000€ anuales. Al ser, un caso académico no se va a pedir precio a los proveedores, debido a que no va a ser un precio realista. Pero con algunos de los precios que se tienen gracias a la referencia mencionada, nos podemos hacer una idea del rango en el que se encuentra.

5.3.3 Requisitos del SIEM para la solución

Los requisitos principales que se deben considerar a la hora de elegir un SIEM (SIEMR) son:

- **SIEMR 1**. El coste de adquisición, mantenimiento y operación del SIEM.

Los SIEM suponen un coste elevado, tanto de adquisición, como de mantenimiento y operación. Por ello es conveniente elegir un SIEM que se ajuste al presupuesto del proyecto.

- **SIEMR 2**. Capacidad de agrupación de diversas fuentes de información.

Es muy importante para un SIEM que sea capaz de agrupar distintas fuentes de información, como las alertas de varios IDS, los logs de algunos de los sistemas que se consideren más críticos u otras fuentes externas. De esta forma, facilitará el trabajo de los analistas de seguridad, dotándoles de la información adecuada para analizar los eventos de seguridad.

5.3.4 Elección de un SIEM para la solución

Para este escenario académico se va a escoger Elastic Stack por dos motivos principales: el bajo coste, incluso gratuito en las capas que se va a usar (cumpliendo SIEMR 1) y porque permite integrar todos los IDS/IPS que se quieran, lo cual cumple con SIEMR 2. Adicionalmente, posee un motor de búsqueda y analítica potente, y permite representar los datos de manera adecuada mediante dashboards (cuadro de mando) y para la creación de informes.

6 IMPLEMENTACIÓN ESCENARIO VIRTUAL

En este apartado se pretende simular la red propuesta en el apartado "5. Arquitectura de red propuesta", con el objetivo de realizar una serie de ataques recogidos en la matriz MITRE y verificar que el sistema de detección de intrusiones funciona correctamente, con el margen de precisión esperado.

6.1 Elección entorno de virtualización

Se ha decidido utilizar Docker para virtualizar el entorno debido a la versatilidad y escalabilidad que ofrece.

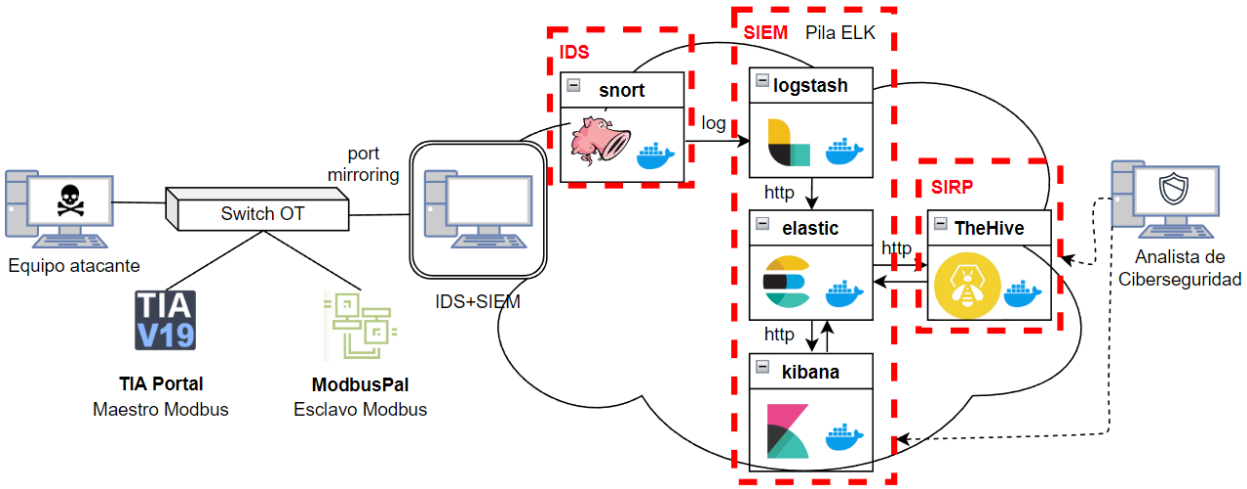

Figura 36. Arquitectura virtual

Los contenedores de cada uno de los servicios se despliegan mediante un Dockercompose, lo cual, simplifica el control de toda la pila de aplicaciones, facilitando la gestión de servicios, redes y volúmenes en un único archivo YAML [81]. El fichero de configuración de cada uno de los servicios se encuentra adjunto en el anexo.

6.2 Virtualización dispositivos

Para simplificar el escenario de las pruebas, los dispositivos que se van a virtualizar son:

- PLC: PLCSim [82]
- Sensores: Modbus PAL [83]
- IDS: Snort se virtualizará sobre Docker
- SIEM: La pila ELK se virtualizará sobre Docker
- SIRP (Security Incident Response Planning): Se trata de un sistema de gestión de las alertas generadas, permite llevar una monitorización de las alertas mediante un sistema de ticketing.

6.3 Escenarios de ataque

Existen múltiples escenarios que se pueden probar basándonos en la matriz MITRE para los Sistemas de Control Industrial (ICS). Para que el Sistema de Detección de Intrusiones (IDS) pueda analizarlos, es necesario que estos ataques cuenten con tráfico de red. Para poder leer los paquetes de red y almacenarlos en los archivos ".pcap", se hará uso de la herramienta wireshark.

El artículo "Exploiting Siemens Simatic S7 PLCs" de la referencia [84], realiza distintos ataques mediante técnicas emergentes a los PLC S7 1200 de Siemens, los cuales se encuentran en la infraestructura que se ha propuesto en el apartado "5.3 Arquitectura de red de comunicaciones". Por lo que junto a algunas técnicas usadas en la referencia "Análisis de la capacidad de detección de Snort sobre ataques de red en ICS bajo la matriz MITRE ATT&CK" [72], se proponen los siguientes escenarios.

6.3.1 Descubrimiento

Las tácticas de descubrimiento consisten en obtener información acerca de la red, los equipos que la componen y como interactúan entre sí. El objetivo es usar esa información para planificar los siguientes movimientos en la red. Se va a hacer uso de la táctica de Descubrimiento de Sistema Remoto, la cual, trata de identificar equipos dentro del entorno de Sistema de Control Industrial. En este caso, identificaremos a los esclavos modbus de la red.

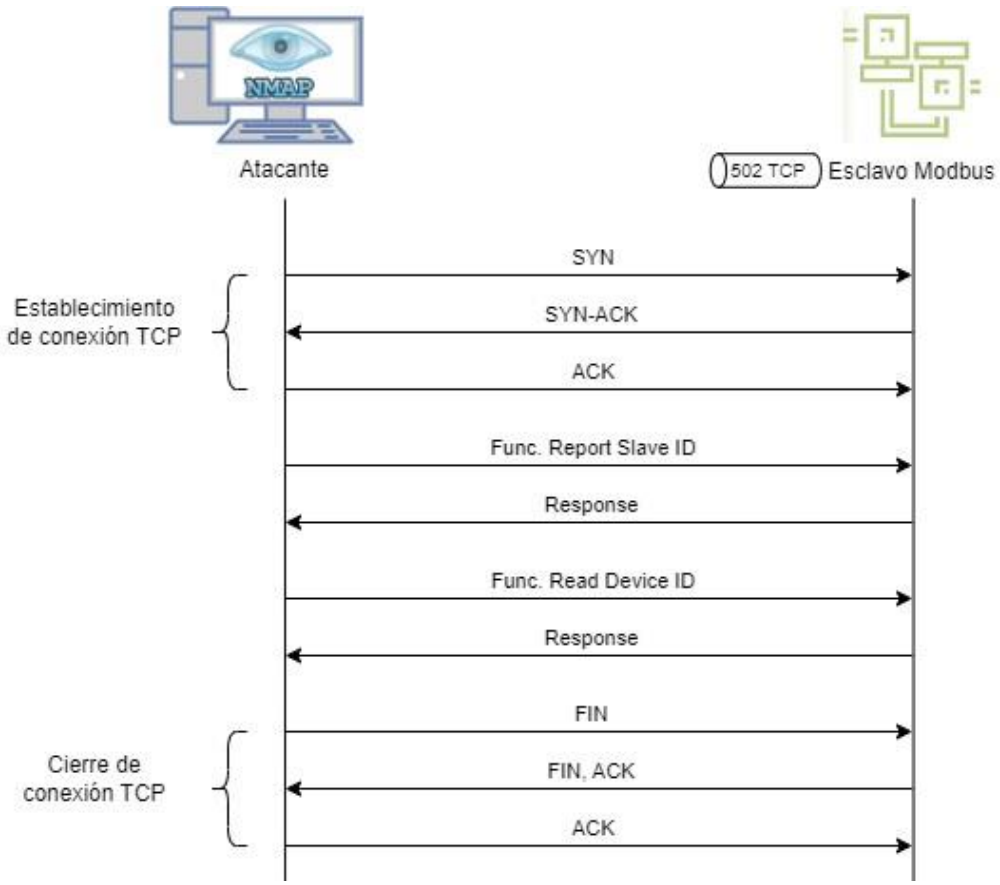

Figura 37. Diagrama de paso de mensajes - Escaneo de equipos que usen Modbus.

6.3.1.1 Configuración de la víctima

Se ejecuta ModbusPal para configurar el equipo esclavo que actuará de víctima.

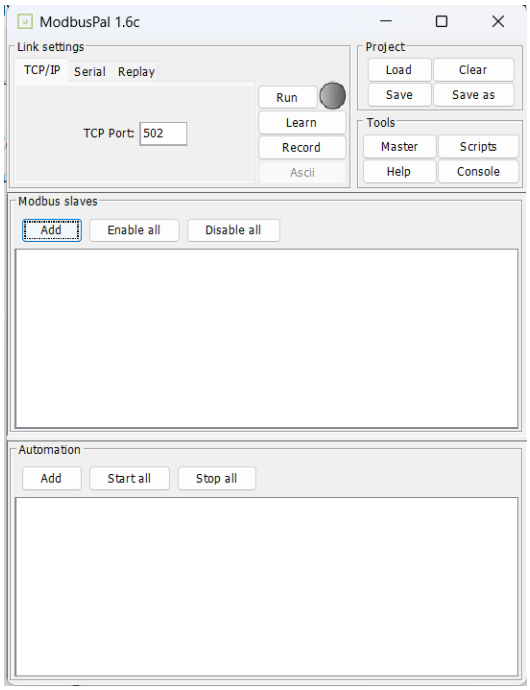

Figura 38. Configuración de esclavo en ModbusPal 1.

Se crea un nuevo esclavo pulsando en el botón Add, aparecerá una nueva ventana en la que se establece el identificador y nombre de este. Después se pulsa el botón Add de la nueva ventana.

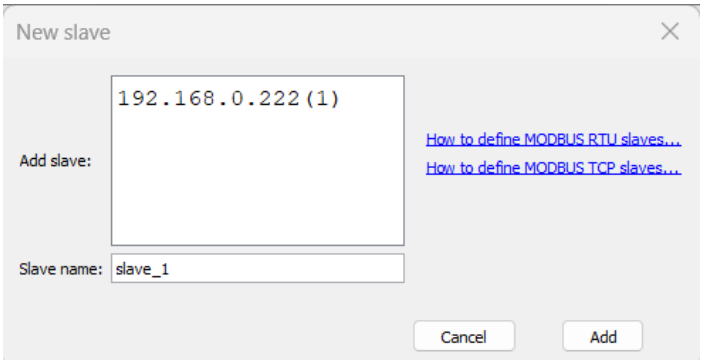

Figura 39. Configuración de esclavo en ModbusPal 2.

A continuación, se crean los registros de almacenamiento del esclavo, pulsando el botón que se muestra en la siguiente figura.

Figura 40. Configuración de esclavo en ModbusPal 3.

Desde la pestaña Holding Registers, se presiona al botón Add y se indica el número de registros de almacenamiento que se desean. Para este caso se seleccionará el máximo, que es 65536.

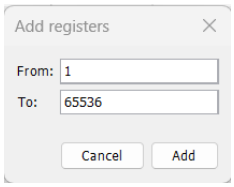

Figura 41. Configuración de esclavo en ModbusPal 4.

Por último, se presiona el botón Run en la ventana principal del programa para que el esclavo se quede esperando peticiones del maestro en el puerto 502 del protocolo TCP.

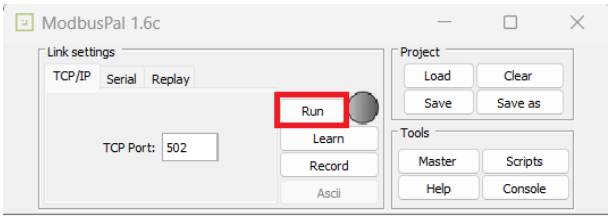

Figura 42. Configuración de esclavo en ModbusPal 5.

6.3.1.2 Configuración del equipo atacante

Se utiliza la herramienta Nmap para escanear la red. Por lo que se requiere configurar una interfaz de red del equipo atacante con una dirección IP en la misma subred que el esclavo Modbus.

6.3.1.3 Ejecución del ataque

Se ejecuta el siguiente comando en el equipo atacante.

```
nmap –script modbus-discover.nse -p 502 192.168.0.222 -Pn
```

La opción “script” permite ejecutar el script especificado, en este caso “`modbus-discover.nse`”. Mediante “-p” elegimos el puerto en el que se desea hacer el escaneo. Con la opción “-Pn”, se indica que no se haga ping previamente a hacer las peticiones Modbus, agilizando el escaneo.

```
PS C:\Users\rober> nmap -p 502 -Pn --script modbus-discover.nse 10.100.154.144
Starting Nmap 7.94 ( https://nmap.org ) at 2024-04-08 09:59 Hora de verano romance
Nmap scan report for 10.100.154.144
Host is up (0.00s latency).

PORT    STATE SERVICE
502/tcp open  modbus
| modbus-discover:
|   sid 0x1:
|_    error: ILLEGAL FUNCTION

Nmap done: 1 IP address (1 host up) scanned in 11.42 seconds
```

Figura 43. Ejecución del ataque de descubrimiento mediante nmap.

6.3.2 Movimiento lateral

Los atacantes tratarán moverse a través de la red, tomando el control de varios dispositivos para llegar al punto deseado de la red. En este apartado se hará uso de la táctica Descarga de Programa, cuyo objetivo es descargar en un equipo remoto un fichero malicioso para que el adversario pueda ganar el control del dispositivo. Se hace uso de la herramienta PLCInjector [85], la cual, permite cargar ficheros en los registros de memoria de un PLC.

Algunos dispositivos como el PLC S7-1200 del Sistema de Control Industrial propuesto en el estudio, ejecutan zonas de memoria de manera periódica, por lo que, si se consiguiera cargar un archivo malicioso en esas zonas de memorias, se podría obtener acceso remoto al mismo.

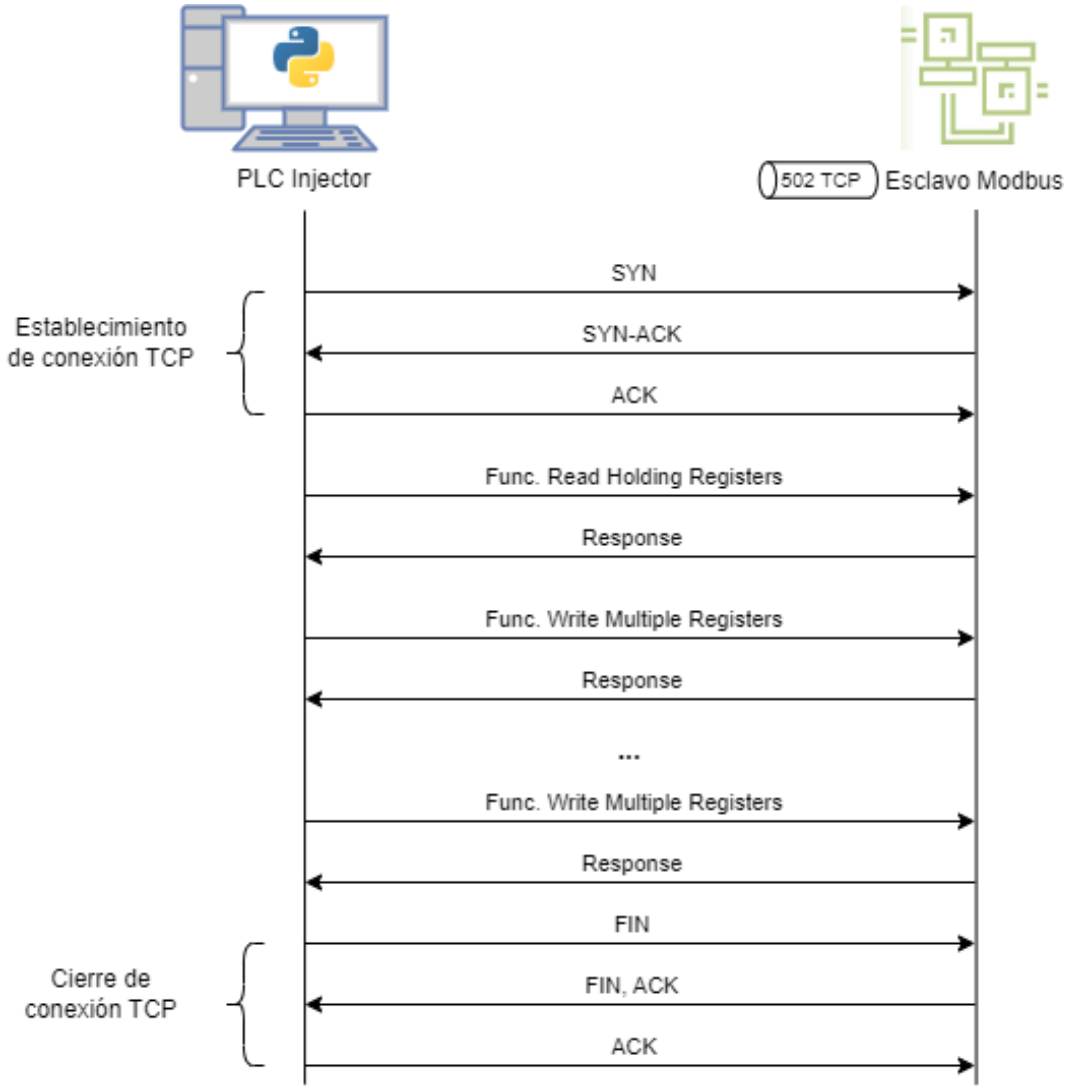

Figura 44. Diagrama paso de mensajes - Movimiento Lateral.

En primer lugar, PLC Injector se encarga de comprobar que hay espacio de memoria suficiente en el equipo víctima para guardar el fichero seleccionado. Para ello hace uso de la función Modbus 0x03, Read Holding Registers. Si determina que puede guardar el archivo, comenzará a mandar mensajes de la función 0x10, Write Multiple Registers, para guardar en la zona de memoria elegida, los datos del fichero.

6.3.2.1 Configuración del equipo víctima

Se toma la misma configuración de partida que en el apartado 8.3.2.1, correspondiente a la táctica de Descubrimiento.

6.3.2.2 Configuración del equipo atacante

Se requiere que el equipo tenga instalado una versión de Python compatible con PLCInjector. Es importante que el equipo atacante configure una de las interfaces de red en la misma subred que el esclavo Modbus.

6.3.2.3 Ejecución del ataque

Los registros del PLC víctima inicialmente están vacíos, como se aprecia en la siguiente figura:

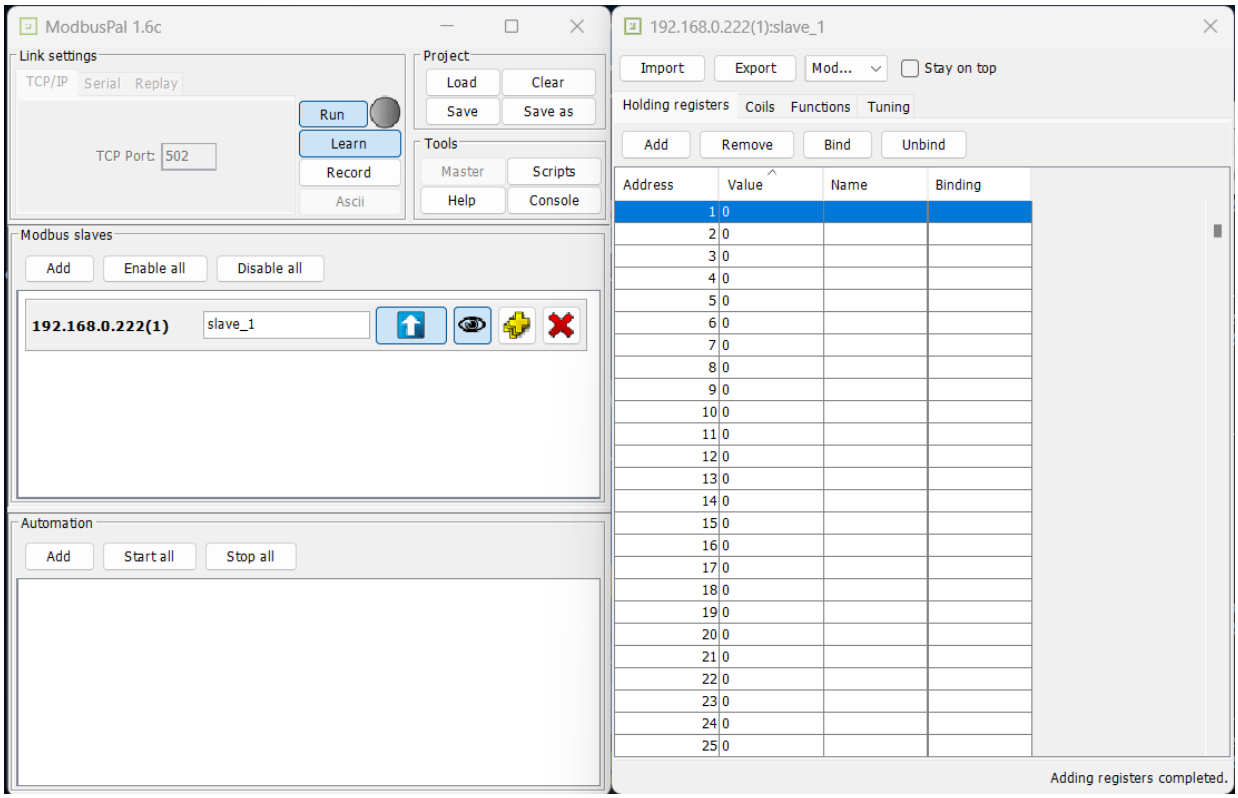

Figura 45. Registros del esclavo Modbus inicialmente - Movimiento Lateral.

Para ejecutar el script del atacante, se hace uso del siguiente comando:

```
python plcInjectPayload.py -upload fichero-malicioso -ip 192.168.0.222
```

En la Figura 46, se muestra el resultado de la ejecución del script anterior.

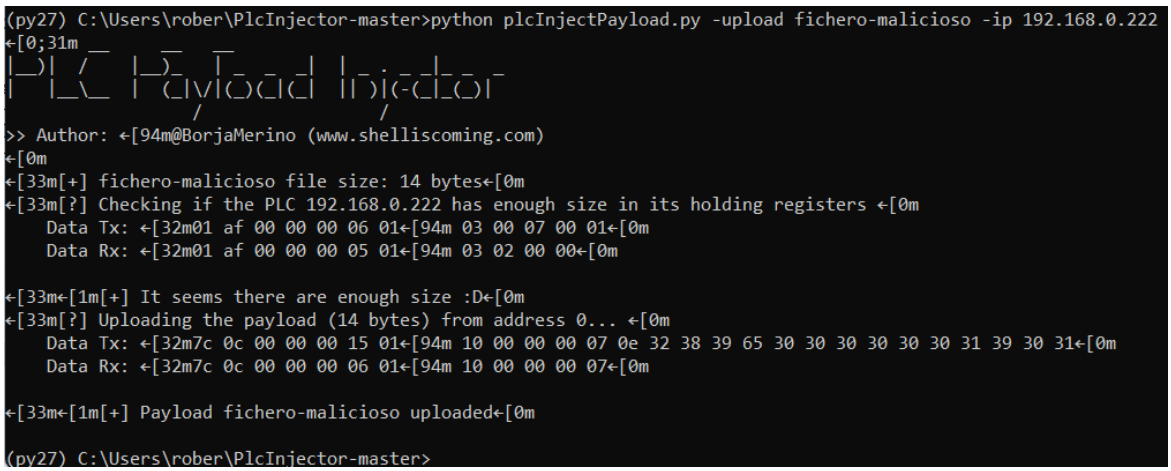

Figura 46. Ejecución de PLCInjector.

Tras la ejecución de PLCInjector, la memoria del dispositivo víctima se aprecia en la Figura 47. Se hace notar que se ha cargado en las primeras direcciones de memoria. En el caso real, se tendría que indicar la posición inicial donde cargar el fichero mediante la opción "-addr".

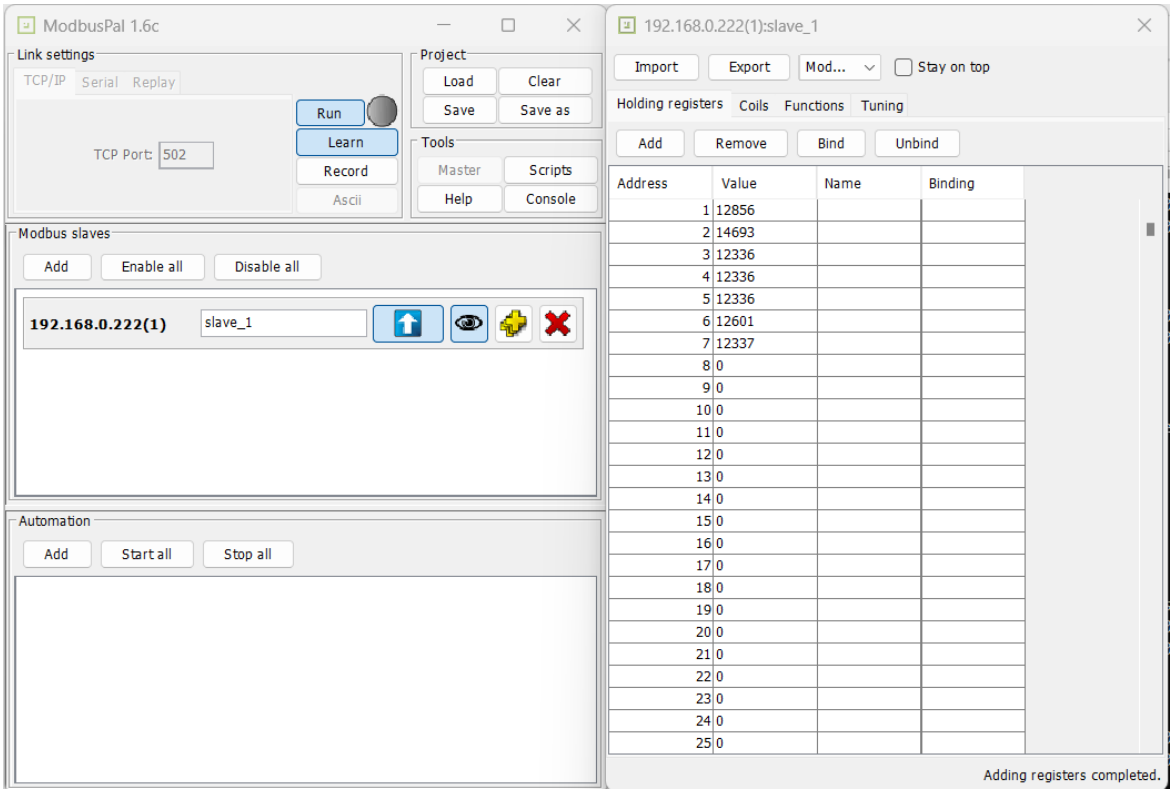

Figura 47. Resultado de la ejecución de PLCInjector.

También se puede descargar el contenido del PLC víctima mediante la opción "-download", lo haría mediante la función "Read Holding Registers".

6.4 Despliegue y uso de la infraestructura

El despliegue de la infraestructura se simplifica mucho debido a que se ha creado un archivo Docker Compose, que permite levantar todos los contenedores preconfigurados con un único comando. La configuración de cada uno de los contenedores se encuentra en el Anexo I.

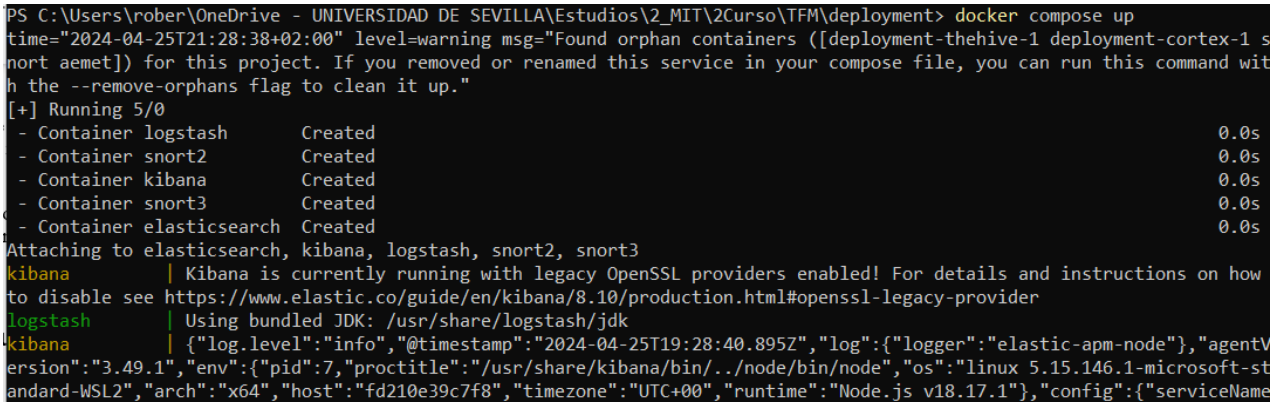

Figura 48. Despliegue de la infraestructura.

En un escenaro real, se configuraría snort para que analizara continuamente el tráfico de una de las interfaces de red mediante la opción "-i". Como se han realizado las pruebas de manera independiente, almacenándolos en pcaps distintos, para una mejor trazabilidad, se ejecutará snort de manera individual para cada uno de los pcaps.

En primer lugar, se entra en el contenedor de snort.

```
docker exec -it snort2 /bin/sh
```

A continuación, se ejecuta snort con el archivo pcap específico a analizar.

Figura 49. Ejecución de snort.

Se puede acceder al servicio de kibana a través del navegador, en la url: http://localhost:5601/. Accediendo al menú de la izquierda y entrando en "Discover", podremos ver los índices configurados y su contenido.

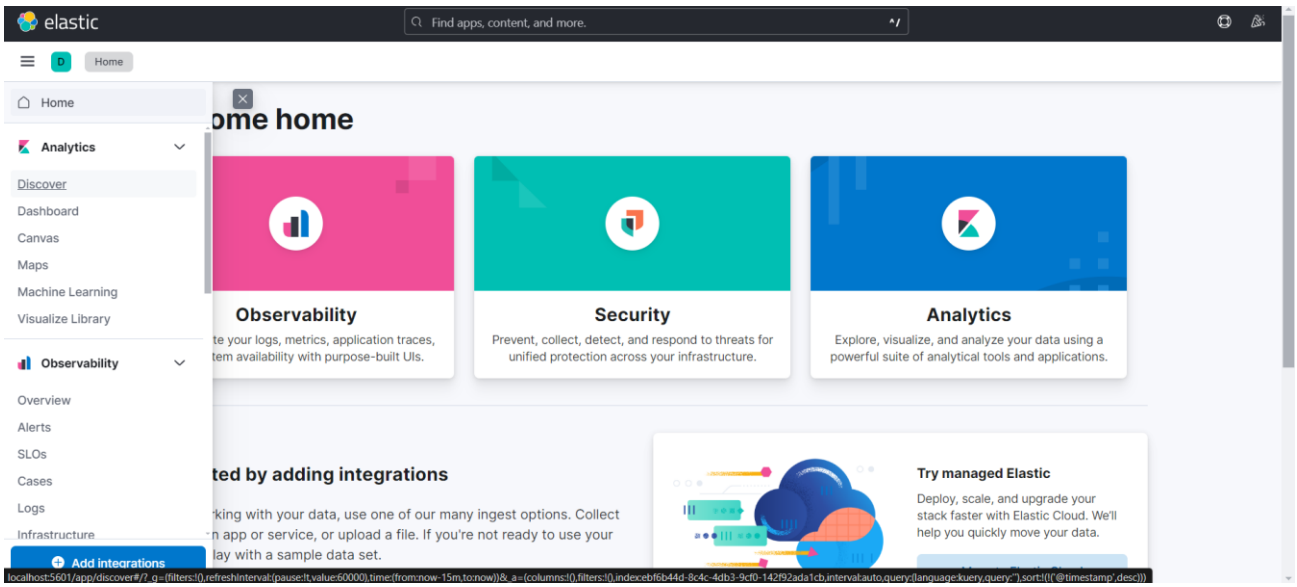

Figura 50. Acceso a Kibana.

En este caso, se observa como se han insertado los documentos en el índice preconfigurado index-snort. Se pueden crear filtros, para poder analizar la información de manera detallada.

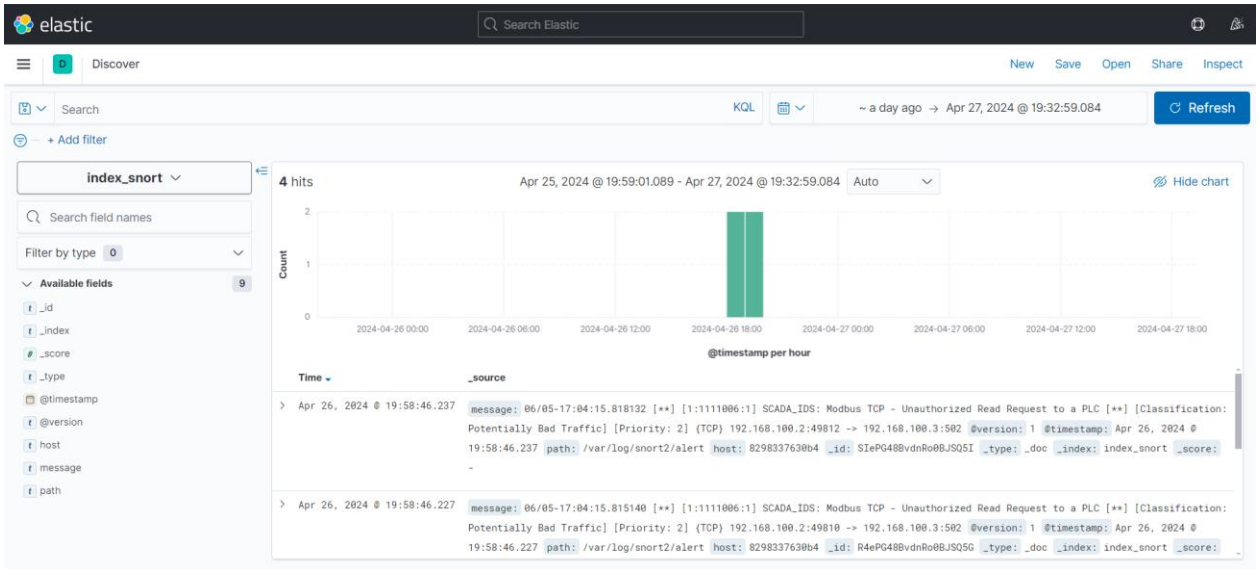

Figura 51. Visualización del índice de snort en Kibana.

Las alertas pasarán a TheHive para que un analista de ciberseguridad las revise, poder asignar técnicos, revisar en cuanto tiempo se ha resuelto la alerta, añadir evidencias y en general, realizar la respuesta al incidente.

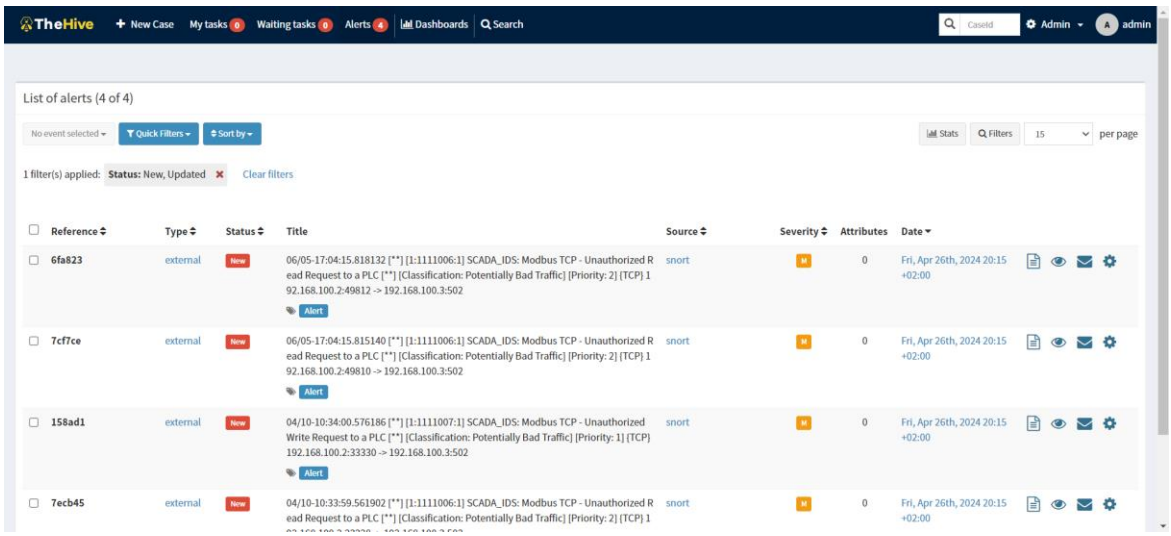

Figura 52. Alertas en TheHive.

En la Figura 53, se aprecia el detalle de una alerta, cuando se hace click sobre ella, mostrando una descripción, los IoC (Indicator of Compromise – Indicador de Compromiso), el título, la fuente de la alerta, las etiquetas, el analista asociado a la alerta…

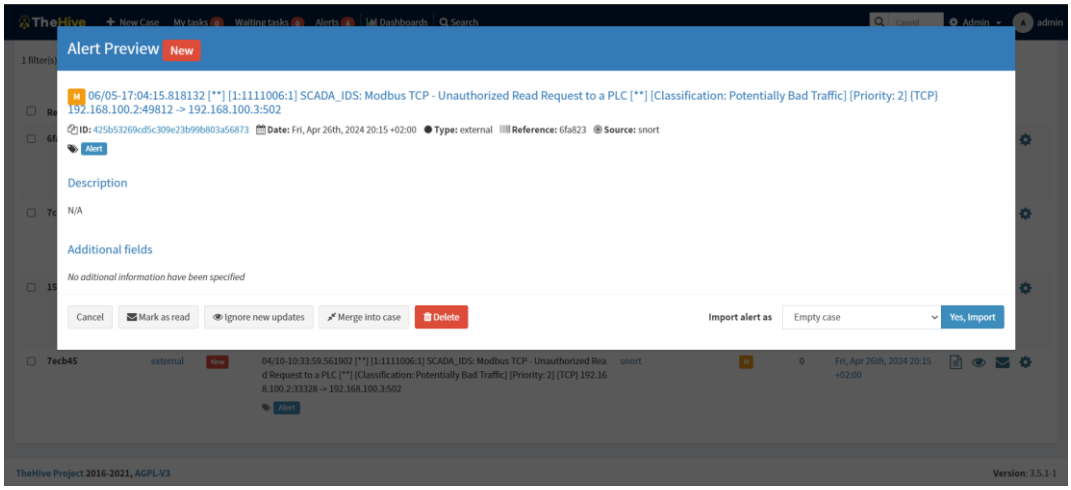

Figura 53. Revisión de una alerta en TheHive.

6.5 Conclusiones de las simulaciones realizadas

Mediante las simulaciones realizadas se puede ver la capacidad de detección del IDS snort de algunas de las tácticas de la matriz MITRE del protocolo Modbus TCP. Cabe destacar que al ser un escenario de prueba y virtualizado, los resultados en un escenario real con los dispositivos físicos podrían variar en cierta medida. Los dos ataques que se han simulado han sido detectados por snort satisfactoriamente y han generado la alerta correspondiente en TheHive.

El objetivo de este apartado de virtualización del escenario ha sido estudiar cómo se realizarían algunos de los ataques de la matriz MITRE, y cómo Snort era capaz de detectarlos, para validar el escenario propuesto para el Plan Director de Ciberseguridad Industrial.

REFERENCIAS

[1] NIST, «Cyber Threat Definition,» 2021. [En línea]. Available: https://csrc.nist.gov/glossary/term/cyber_threat.

[2] CTN 203 Equipamiento eléctrico y sistemas automáticos para la industria, «UNE-EN IEC 62443-3-3: Redes de comunicaciones industriales. Seguridad de la red y del sistema. Parte 3-3: Requisitos de seguridad del sistema y niveles de seguridad,» 2020.

[3] proofpoint, «Definición modelo OSI,» [En línea]. Available: https://www.proofpoint.com/es/threat-reference/osi-model.

[4] IBM, «Security Operations Center,» 2024. [En línea]. Available: https://www.ibm.com/topics/security-operations-center.

[5] INCIBE, «Estudio del análisis de malware en SCI, BlackEnergy,» 2024. [En línea]. Available: https://www.incibe.es/incibe-cert/blog/estudio-del-analisis-de-malware-en-sci-blackenergy.

[6] AENOR, «Norma UNE EN ISO IEC 27001,» 2017. [En línea]. Available: https://www.industriaconectada40.gob.es/difusion/Documents/Documento_Norma_UNE-EN_ISO-IEC_27001%20MINTUR.pdf.

[7] I. G. C. Alliance, «Applying ISO/IEC 27001/2 and the ISA/IEC 62443 Series for Operational Technology Environments,» [En línea]. Available: https://gca.isa.org/applying-iso/iec-27001/2-and-the-isa/iec-62443-series-for-operational-technology-environments.

[8] CTN 203 Equipamiento eléctrico y sistemas automáticos para la industria, «UNE-EN IEC 62443-3-2. Evaluación del riesgo de seguridad para el diseño de sistemas,» 2021.

[9] ISA Global Cybersecurity Alliance, «Quick Start Guide: An Overview of ISA/IEC 62443 Standards,» [En línea]. Available: https://isagca.org/isa-iec-62443-standards.

[10] UNE, UNE-EN IEC 62351-3:2023: Gestión de sistemas de potencia e intercambio de información asociada. Seguridad de datos y comunicaciones Parte 3: Seguridad del sistema y de la red de comunicación. Perfiles incluyendo TCP/IP, 2023.

[11] A. Valencia, «¿Cómo es un incidente de ciberseguridad industrial?,» 24 3 2023. [En línea]. Available: https://www.cci-es.org/como-es-un-incidente-de-ciberseguridad-industrial/.

[12] BBC, «El virus que tomó control de mil máquinas y les ordenó autodestruirse,» 2015. [En línea]. Available: https://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet.

[13] HHS, «Types Threat Actors Healthcare,» 2023. [En línea]. Available: https://www.hhs.gov/sites/default/files/types-threat-actors-threaten-healthcare.pdf.

[14] Electronic Transactions Development Agency, «Hexane,» 2024. [En línea]. Available: https://apt.etda.or.th/cgi-bin/showcard.cgi?g=Hexane.

[15] Electronic Transactions Development Agency, «Lockbit,» 2024. [En línea]. Available: https://apt.etda.or.th/cgi-bin/showcard.cgi?g=LockBit%20Gang.

[16] Electronic Transactions Development Agency, «APT group: APT 33, Elfin, Magnallium,» 2024. [En línea]. Available: https://apt.etda.or.th/cgi-bin/showcard.cgi?g=APT%2033%2C%20Elfin%2C%20Magnallium.

[17] Electronic Transactions Development Agency, «Lapsus$,» 2024. [En línea]. Available: https://apt.etda.or.th/cgi-bin/showcard.cgi?g=Lapsus%24.

[18] HHS, «Pro-Russian Hacktivist Group 'KillNet' Threat to HPH Sector,» 2022. [En línea]. Available: https://www.hhs.gov/sites/default/files/killnet-analyst-note-tlpclear.pdf.

[19] Electronic Transactions Development Agency, «Operation Olympic Games,» 2024. [En línea]. Available: https://apt.etda.or.th/cgi-bin/showcard.cgi?g=Operation%20Olympic%20Games.

[20] The New York Times, «Obama Ordered Wave Of Cyberattacks Against Iran,» 2012. [En línea]. Available: https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html.

[21] Electronic Transactions Development Agency, «Lazarus Group, Hidden Cobra, Labyrinth Chollima,» 2024. [En línea]. Available: https://apt.etda.or.th/cgi-bin/showcard.cgi?g=Lazarus%20Group%2C%20Hidden%20Cobra%2C%20Labyrinth%20Chollima.

[22] Electronic Transactions Development Agency, «Wicked Panda,» 2024. [En línea]. Available: https://apt.etda.or.th/cgi-bin/showcard.cgi?g=Winnti%20Group%2C%20Wicked%20Panda.

[23] Accenture, «New Report Finds Insider Corporate Data Theft and Malware Infections Among Biggest Threat to Digital Business in 2016,» 2016. [En línea]. Available: https://newsroom.accenture.com/news/2016/new-report-finds-insider-corporate-data-theft-and-malware-infections-among-biggest-threat-to-digital-business-in-2016.

[24] CCI, «Ciberseguridad Industrial Esencial,» [En línea]. Available: https://www.cci-es.org/ciberseguridad-industrial-esencial/.

[25] E. Csanyi, «Five terms you must be familiar with: SCADA, DCS, PLC and Smart Instrument,» Electrical Engineering Portal, [En línea]. Available: https://electrical-engineering-portal.com/scada-dcs-plc-rtu-smart-instrument. [Último acceso: 2024].

[26] J. Nideborn, «HMS Networks,» 7 5 2019. [En línea]. Available: https://www.hms-networks.com/news-and-insights/news-from-hms/2019/05/07/industrial-network-market-shares-2019-according-to-hms#:~:text=Industrial%20Ethernet%20now%20accounts%20for,of%20the%20market%20(6).

[27] M. Herrero Collantes y A. López Padilla, «Protocols and Network Security in ICS Infrastructures,» 2017.

[28] Cloudflare, «What is SSL?,» [En línea]. Available: https://www.cloudflare.com/es-es/learning/ssl/what-is-ssl.

[29] D. Ehrenreich, «SRP Triad -Best for ICS Cyber Security,» 2018. [En línea]. Available: https://www.linkedin.com/pulse/srp-triad-best-ics-cyber-security-daniel-ehrenreich/.

[30] T. Cornelius, «The "CIA Triad" Is Insufficient In The Age of AI/OT/IoT,» 2023. [En línea]. Available: https://www.linkedin.com/pulse/cia-triad-insufficient-age-aiotiot-tom-cornelius/.

[31] NIST, «Cyber Attack Definition,» 2021. [En línea]. Available: https://csrc.nist.gov/glossary/term/cyber_attack.

[32] P. Radoglou Grammatikis, P. Sarigiannidis, I. Giannoulakis, E. Kafetzakis y E. Panaousis, «Attacking IEC-60870-5-104 SCADA Systems,» *IEEE,* 2019.

[33] MITRE, «Matriz ICS,» 2024. [En línea]. Available: https://attack.mitre.org/matrices/ics/.

[34] INCIBE, «Matriz Mitre: Tácticas y técnicas en entornos industriales,» 2022. [En línea]. Available: https://www.incibe.es/incibe-cert/blog/matriz-mitre-tacticas-y-tecnicas-entornos-industriales.

[35] Deloitte, «Ciberseguridad en el sector electrico,» [En línea]. Available: https://www2.deloitte.com/content/dam/Deloitte/co/Documents/risk/cl-ciberseguridad-en-el-sector-electrico-diciembre-2020.pdf.

[36] ICSCSI, «ICS Cyber Kill Chain,» 2015. [En línea]. Available: https://icscsi.org/library/Documents/White_Papers/SANS%20-%20ICS%20Cyber%20Kill%20Chain.pdf.

[37] INCIBE, «Plan Director de Seguridad,» 2020. [En línea]. Available: https://www.incibe.es/empresas/que-te-interesa/plan-director-seguridad.

[38] INCIBE, «Hacker vs Ciberdelincuente,» [En línea]. Available: https://www.incibe.es/aprendeciberseguridad/hacker-vs-ciberdelincuente. [Último acceso: 2024].

[39] RAE, «Definición de Estado,» [En línea]. Available: https://dle.rae.es/estado. [Último acceso: 2024].

[40] RAE, «Definición de terrorismo,» [En línea]. Available: https://dpej.rae.es/lema/terrorismo#:~:text=Provocaci%C3%B3n%20o%20mantenimiento%20en%20estado,la%20conservaci%C3%B3n%20de%20los%20bienes. [Último acceso: 2024].

[41] CCN CERT, «Amenazas y análisis de riesgos en Sistemas de Control Industrial,» 2016. [En línea]. Available: https://www.ccn-cert.cni.es/gl/pdf/informes-de-ciberseguridad-ccn-cert/informes-ccn-cert-publicos/1381-ccn-cert-ia-04-16-amenazas-y-analisis-de-riesgos-en-sistemas-de-control-industrial-ics/file.html.

[42] Proofpoint, «Definición de agente de amenazas,» [En línea]. Available: https://www.proofpoint.com/es/threat-reference/threat-actor#:~:text=Un%20agente%20de%20amenaza%20es,una%20vulnerabilidad%20o%20creando%20malware..

[43] S. Koelemij, «OT Cyber Security Risk,» 2020. [En línea]. Available: https://otcybersecurity.blog/2020/06/14/ot-cyber-security-risk/.

[44] CSA Singapore, «GUIDE TO CONDUCTING CYBERSECURITY RISK ASSESSMENT FOR CRITICAL INFORMATION INFRASTRUCTURE,» 2021. [En línea]. Available: https://www.csa.gov.sg/docs/default-source/csa/documents/legislation_supplementary_references/guide-to-conducting-cybersecurity-risk-assessment-for-cii.pdf?sfvrsn=a63bf6d8_0.

[45] INCIBE, «Proceso de certificación en IEC62443,» [En línea]. Available: https://www.incibe.es/incibe-

cert/blog/el-proceso-de-certificacion-en-iec62443-3-3.

[46] ICS-CERT, «Seven Strategies to Defend ICSs,» 2015. [En línea]. Available: https://www.cisa.gov/sites/default/files/documents/Seven%20Steps%20to%20Effectively%20Defend%20Industrial%20Control%20Systems_S508C.pdf.

[47] J. D. Hidalgo Quesada, Guía Básica de Diseño de Subestaciones Eléctricas con Énfasis en el Arreglo de Barras Colectoras de Interruptor y Medio, 2008.

[48] Kaspersky, «Ciberseguridad para infraestructuras eléctricas,» 2017. [En línea]. Available: https://content.kaspersky-labs.com/se/media/es/business-security/enterprise/kl-industrial-cybersecurity-for-energy.pdf.

[49] Iberdrola, Reglamento sobre centrales eléctricas, subestaciones y centros de transformación, 2022.

[50] D. Dolezilek, D. Gammel y W. Fernandes, «CYBERSECURITY BASED ON IEC 62351 AND IEC 62443 FOR IEC 61850 SYSTEMS,» 2020. [En línea]. Available: https://selinc.com/api/download/130122/?lang=en.

[51] INCIBE, «Mejorando la seguridad del IEC 104 con ayuda del estándar IEC 62351,» 2018. [En línea]. Available: https://www.incibe.es/incibe-cert/blog/mejorando-seguridad-del-iec-104-ayuda-del-estandar-iec-62351.

[52] C. MONTES PORTELA, M. HOEVE, F. Hwa TAN y H. SLOOTWEG, «IMPLEMENTING AN ISA/IEC-62443 AND ISO/IEC-27001 OT CYBER SECURITY MANAGEMENT SYSTEM AT DUTCH DSO ENEXIS,» 2019. [En línea]. Available: https://www.cired-repository.org/server/api/core/bitstreams/f8b15769-4248-4d9a-9b7a-81681b39a71a/content.

[53] S. F. y S. , «Cybersecurity in Power Systems: A view on regulation and standardization,» 2023. [En línea]. Available: https://www.iaria.org/conferences2023/filesENERGY23/SteffenFries_Keynote_CybersecurityInPower.pdf.

[54] J. G. Mar Perez, Descripción y Función del Equipo de una Subestación Eléctrica, 2011.

[55] G. E. «Constitución de los sistemas eléctricos,» 2013. [En línea]. Available: https://globalelectricity.wordpress.com/2013/10/31/constitucion-de-los-sistemas-electricos/.

[56] C. A. Báez Rivera y C. D. León Guerrero, Diseño e implementación de un sistema SCADA complementario para control y monitoreo de la subestación de San Gabriel, Universidad de las fuerzas armadas, 2016.

[57] S. Cárdenas Tapia y P. Moreno Gutiérrez, «Implementación de la subestación Vilcamba al sistema SCADA de la Empresa Eléctrica Regional del Sur S.A, Segunda etapa. LOJA,» 2011. [En línea]. Available: https://dspace.ups.edu.ec/bitstream/123456789/1453/13/UPS-CT002332.pdf.

[58] J. d. C. y. L. «Energía y minería en Castilla y León,» [En línea]. Available: https://energia.jcyl.es/web/es/biblioteca/suministro-electricidad-aplicaciones.html#:~:text=En%20la%20industria%2C%20casi%20la,de%20tanques%2C%20dep%C3%B3sitos%20o%20calderas..

[59] C. A. Báez Rivera y C. D. León Guerrero, DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA SCADA

COMPLEMENTARIO PARA CONTROL Y MONITOREO DE LA SUBESTACIÓN ELÉCTRICA SAN GABRIEL, UNIVERSIDAD DE LAS FUERZAS ARMADAS, ECUADOR, 2016.

[60] E. Gamess, B. Smith y G. A. Francia lii, «Performance Evaluation of Modbus TCP in Normal Operation and Under A Distributed Denial of Service Attack,» *International Journal of Computer Networks and Communications,* 2020.

[61] Modbus, «Modbus Application Protocol V1,» 2006. [En línea]. Available: https://modbus.org/docs/Modbus_Application_Protocol_V1_1b.pdf.

[62] INCIBE, «Diseño y Configuración de IPS, IDS y SIEM en Sistemas de Control Industrial,» 2017. [En línea]. Available: https://www.incibe.es/sites/default/files/contenidos/guias/doc/certsi_diseno_configuracion_ips_ids_siem_en_sci.pdf.

[63] INCIBE, «Soluciones IDS en entornos industriales,» 2023. [En línea]. Available: https://www.incibe.es/incibe-cert/blog/soluciones-ids-en-entornos-industriales.

[64] ivanti, «Deployment od IPS with SCADAguardian,» 2022. [En línea]. Available: https://help.ivanti.com/ps/help/en_US/PPS/9.1R14/int-nozomi/deployment_of_ips_with_nozomi_networks_scadaguardian.htm.

[65] IBM Security, «IBM QRadar and Nozomi Networks SCADAguardian,» [En línea]. Available: https://uploads-ssl.webflow.com/645a4534705010e2cb244f50/64c9b36645eaffe3500c9f81_IBM-QRadar-Nozomi-Networks-OT-IT-Visibility.pdf.

[66] S2 GRUPO, «GLORIA ICS,» 2024. [En línea]. Available: https://s2grupo.es/herramientas/gloria-ics/.

[67] Nozomi Networks, «SG Data Sheet,» [En línea]. Available: https://www.servitecno.it/wp-content/uploads/2018/01/Nozomi-Networks-SG-Data-Sheet.pdf.

[68] OISF, «Reglas y decodificadores suricata,» 2024. [En línea]. Available: https://github.com/OISF/suricata/tree/master/rules.

[69] Palo Alto Networks, «Learn device attributes by polling,» 2024. [En línea]. Available: https://docs.paloaltonetworks.com/iot/iot-security-integration/asset-discovery/learn-device-attributes-by-polling.

[70] digitalbond, «Digital Bond's IDS/IPS rules for ICS and ICS protocols,» 2020. [En línea]. Available: https://github.com/digitalbond/Quickdraw-Snort/tree/master.

[71] IBM, «QRadar Admin Guide,» [En línea]. Available: https://www.ibm.com/docs/es/SSKMKU/com.ibm.qradar.doc/b_qradar_admin_guide.pdf.

[72] P. Benítez Sánchez, «Análisis de la capacidad de detección de Snort sobre ataques de red en ICS bajo la matriz MITRE ATT&CK,» *Universidad de Sevilla,* 2022.

[73] INCIBE, «Despliegue de un SIEM en entornos industriales,» 2019. [En línea]. Available: https://www.incibe.es/incibe-cert/blog/despliegue-de-siem-en-entornos.

[74] P. F. Nacimba Loachamín, «ANÁLISIS COMPARATIVO DE PLATAFORMAS DE SIEM Y LAS SOLUCIONES,» 2021. [En línea]. Available: https://repositorio.uisrael.edu.ec/xmlui/bitstream/handle/47000/3558/UISRAEL-EC-MASTER-SEG-

INF%20-378.242-2023-006.pdf?sequence=1&isAllowed=y.

[75] Fortinet, «FortiSIEM,» 2024. [En línea]. Available: https://www.fortinet.com/lat/products/siem/fortisiem.

[76] IT Price, «Fortinet FortiSIEM price list,» 2024. [En línea]. Available: https://itprice.com/fortinet-price-list/siem.html.

[77] Microsoft, «Sentinel Pricing,» 2024. [En línea]. Available: https://azure.microsoft.com/en-us/pricing/details/microsoft-sentinel/.

[78] Digital Marketplace Gov UK, «Nozomi Guardian,» 2024. [En línea]. Available: https://www.applytosupply.digitalmarketplace.service.gov.uk/g-cloud/services/337303041784164.

[79] À. Rigau Pedraza, «Ventajas e implementación de un sistema SIEM,» *Universitat Oberta de Catalunya.*

[80] SelectHub, «Comparativo Herramientas SIEMs,» 2024. [En línea]. Available: https://www.selecthub.com/c/siem-tools/.

[81] Docker , «Docker Compose,» [En línea]. Available: https://docs.docker.com/compose/. [Último acceso: 2024].

[82] Siemens, «Descarga del SIMATIC STEP 7, incluyendo Safety, S7-PLCSIM y WinCC V19 de prueba (trial),» 2023. [En línea]. Available: https://support.industry.siemens.com/cs/document/109820994/descarga-del-simatic-step-7-incluyendo-safety-s7-plcsim-y-wincc-v19-de-prueba-(trial)?dti=0&lc=es-WW.

[83] modbuspal, «ModbusPAL,» [En línea]. Available: https://modbuspal.sourceforge.net/ . [Último acceso: 2024].

[84] B. Dillon, «Exploiting Siemens Simatic S7 PLCs,» 2011.

[85] B. Merino, «PLCInjector,» [En línea]. Available: https://github.com/BorjaMerino/PlcInjector.

[86] INCIBE, «Análisis de riesgos,» 2017. [En línea]. Available: https://www.incibe.es/empresas/blog/analisis-riesgos-pasos-sencillo#:~:text=C%C3%A1lculo%20del%20riesgo,RIESGO%20%3D%20PROBABILIDAD%20x%20IMPACTO..

[87] C. Forge, «Confidentiality, Integrity, Availability & Safety (CIAS) Model,» 2017. [En línea]. Available: https://complianceforge.com/free-guides/confidentiality-integrity-availability-security-cias.

[88] M. Souppaya y K. Scarfone, «NIST Special Publication 800-83,» 2013. [En línea]. Available: https://csrc.nist.gov/glossary/term/malware#:~:text=NIST%20SP%20800%2D61%20Rev,%2C%20applications%2C%20or%20operating%20system..

[89] K. Stouffer , V. Pillitteri , S. Lightman , M. Abrams y A. Hahn , «NIST Special Publication (SP) 800-82 Revision 2,» [En línea]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf.

[90] CIGRE, «Plan Director de Ciberseguridad Para el Sector Eléctrico,» [En línea]. Available: https://www.cigre.cl/pdf/PDC/PlanDirector-Ciberseguridad-CIGRE-ES.pdf.

[91] AENOR, «UNE EN ISO IEC 27002,» 2017. [En línea]. Available: https://www.industriaconectada40.gob.es/difusion/Documents/Documento_Norma_UNE-EN_ISO-IEC_27002_MINTUR.pdf.

[92] SIA, «Barómetro SIA 2023. Ciberseguridad OT: Energía. Proteger la operación, los costes y la reputación en los entornos de operación,» 2023. [En línea].

[93] Diverxia Infrastructure, «Proyecto de Ejecución de la Subestación 220/30kV,"Venalta",» 2018. [En línea]. Available: https://www.juntadeandalucia.es/sites/default/files/2020-10/PRO18-06-001_PROYECTO%20COMPLETO_Venalta_rev01_sgd.pdf.

[94] ClearSky, «Lyceum suic 23.06.2022 ide drone,» 2023. [En línea]. Available: https://www.clearskysec.com/wp-content/uploads/2022/06/Lyceum-suicide-drone-23.6.pdf.

[95] Electronic Transactions Development Agency, «APT group: TEMP.Veles,» 2022. [En línea]. Available: https://apt.etda.or.th/cgi-bin/showcard.cgi?g=TEMP%2EVeles.

[96] Electronic Transactions Development Agency, «Allanite,» 2022. [En línea]. Available: https://apt.etda.or.th/cgi-bin/showcard.cgi?g=Allanite.

[97] Electronic Transactions Development Agency, «Covellite,» 2021. [En línea]. Available: https://apt.etda.or.th/cgi-bin/showcard.cgi?g=Covellite.

[98] Electronic Transactions Development Agency, «FIN11,» 2024. [En línea]. Available: https://apt.etda.or.th/cgi-bin/showcard.cgi?g=FIN11.

[99] M. A. Toscano Palacios, Automatización de una Subestación Eléctrica utilizando el protocolo IEC 61850 y el ICCP para el envío de Datos, Universidad Ricardo Palma, 2010.

Anexo I : Instalación y configuración de herramientas

I.1. TIA Portal

I.1.1. Creación de un nuevo proyecto

Tras abrir el programa aparecerá la siguiente pantalla, en la que deberemos establecer un nombre y ubicación de proyecto.

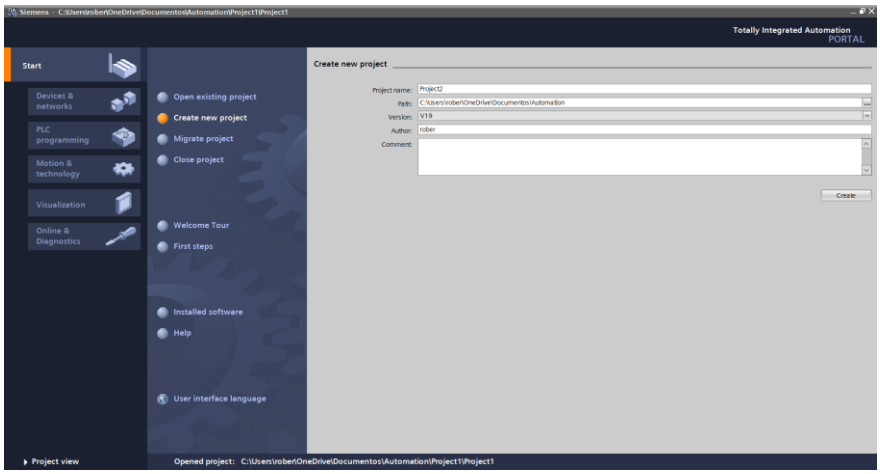

Figura 54. Creación proyecto TIA Portal 1.

A continuación, seleccionamos la opción “Open the Project view”.

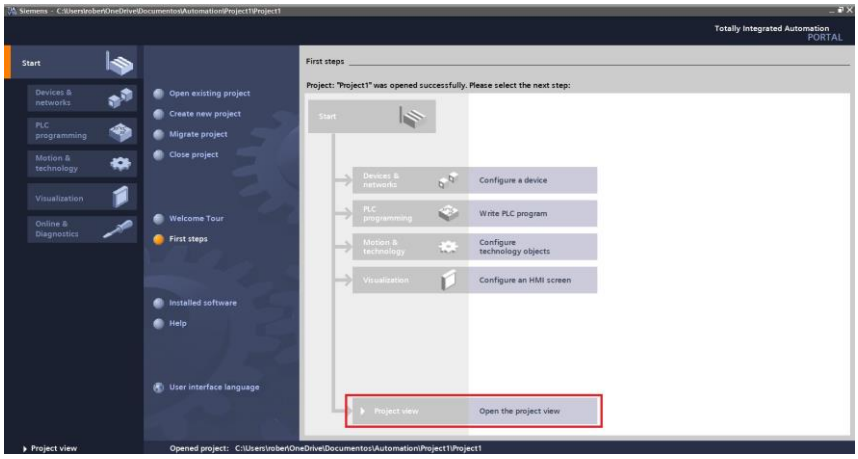

Figura 55. Creación proyecto TIA Portal 2.

Posteriormente, seleccionamos el dispositivo CPU 1214C DC/DC/DC versión V4.6.

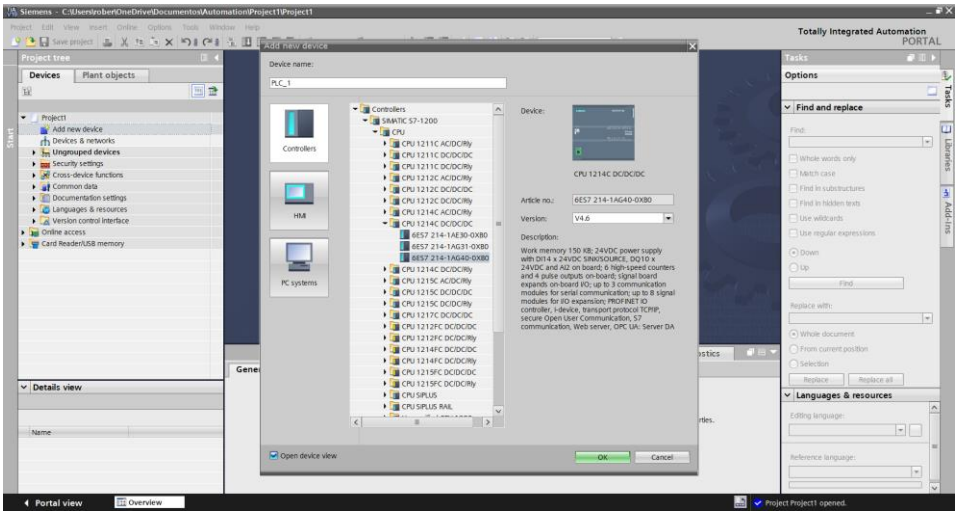

Figura 56. Creación proyecto TIA Portal 3.

Dejamos la opción por defecto y pasamos a la siguiente pantalla.

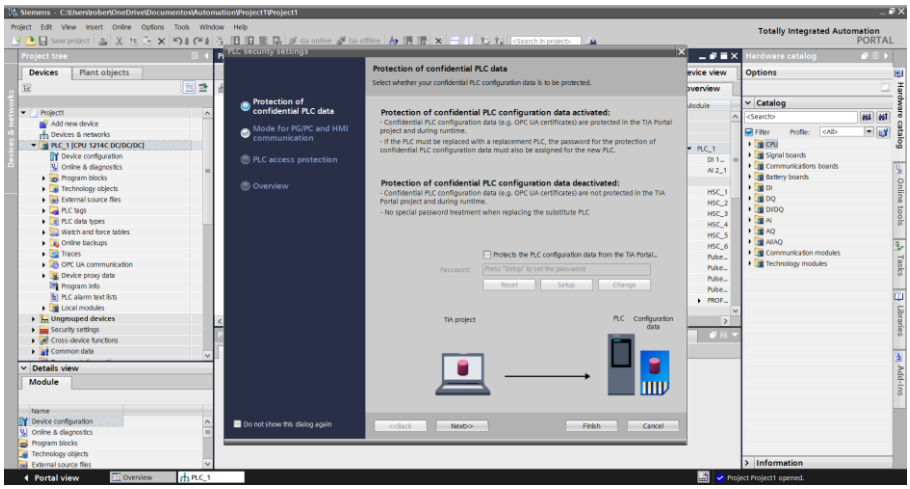

Figura 57. Creación proyecto TIA Portal 4.

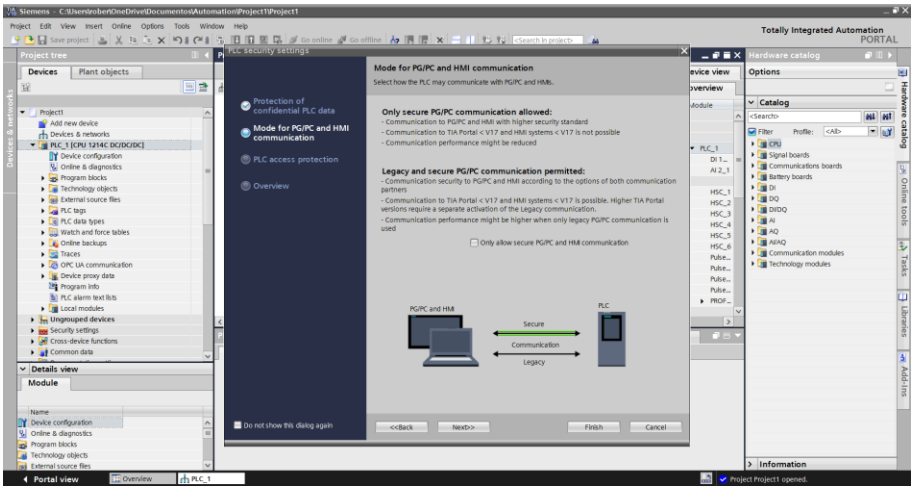

Figura 58. Creación proyecto TIA Portal 5.

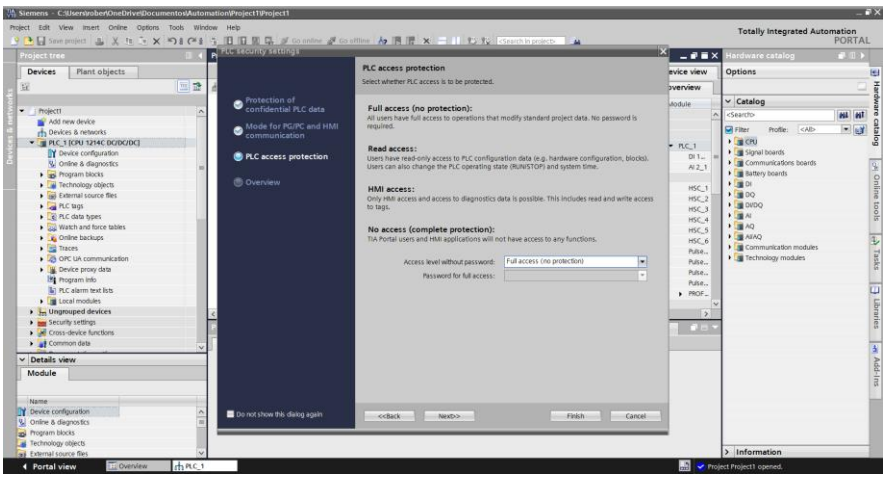

Figura 59. Creación proyecto TIA Portal 6.

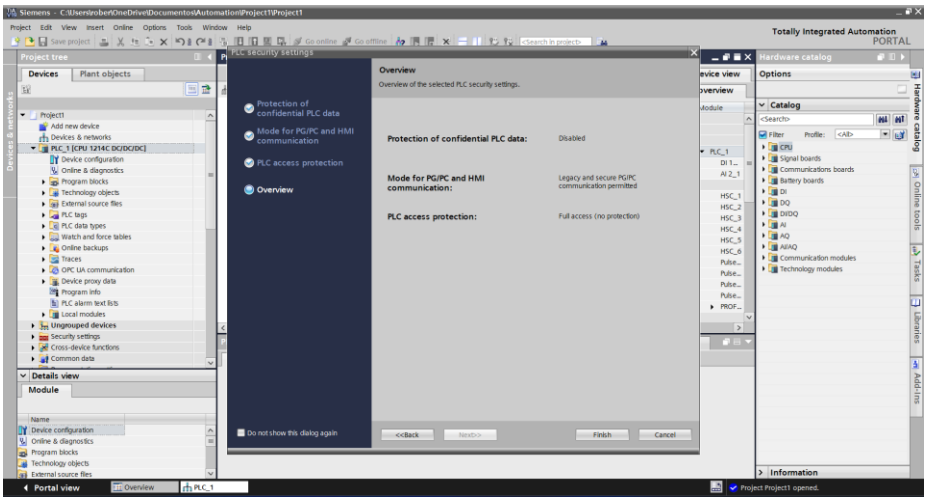

Figura 60. Creación proyecto TIA Portal 7.

Establecemos la dirección IP del dispositivo, en este caso, 192.168.0.225/24.

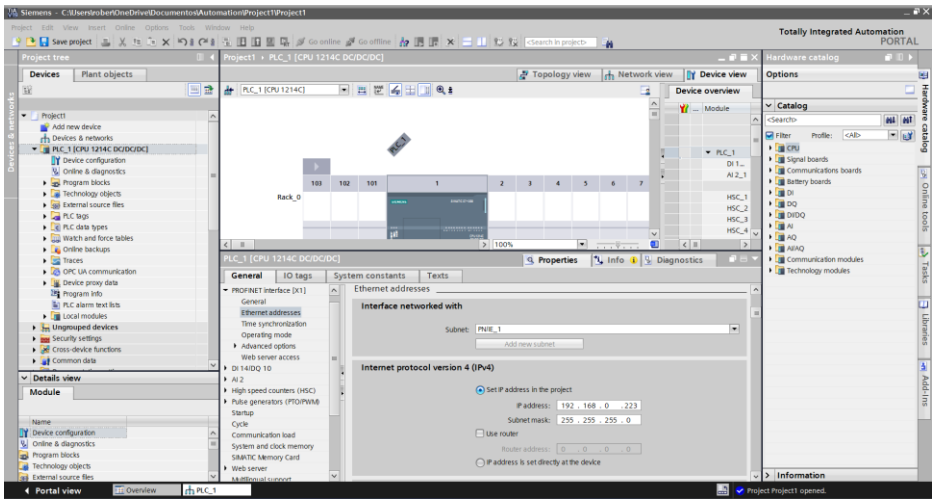

Figura 61. Creación proyecto TIA Portal 8.

Se compila el PLC pulsando el siguiente icono.

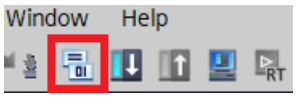

Figura 62. Compilación del PLC.

Se debe obtener el siguiente resultado de la compilación.

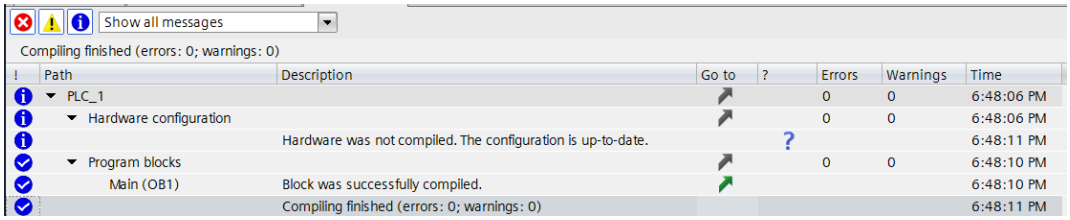

Figura 63. Resultado de la compilación.

Después, se carga la configuración en el PLC simulado.

Figura 64. Carga de configuración en el PLC simulado.

I.1.2. Configuración de la interfaz de red para TIA Portal

Se activa el servicio de NetGroup Packet Filter mediante el siguiente comando

```
PS C:\WINDOWS\system32> net start npf

El servicio de NetGroup Packet Filter Driver se ha iniciado correctamente.
```

Figura 65. Configuración red TIA Portal 1.

Se abre el programa PLCSIM Advanced y se activa la interfaz Ethernet virtual.

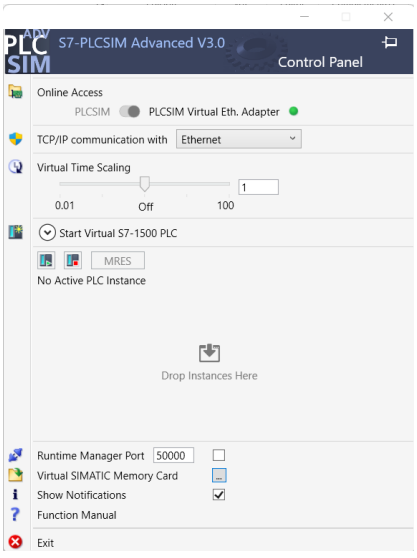

Figura 66. Configuración red TIA Portal 2

I.1.3. Configurar Modbus Server en TIA Portal

Se crea una base de datos para la información de Modbus.

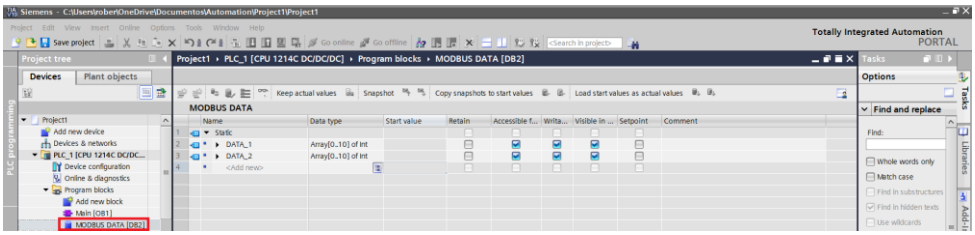

Figura 67. Configurar Modbus Server en TIA Portal 1.

Click derecho en la nueva base de datos creada, y se selecciona propiedades. Se desactiva el acceso optimizado al bloque.

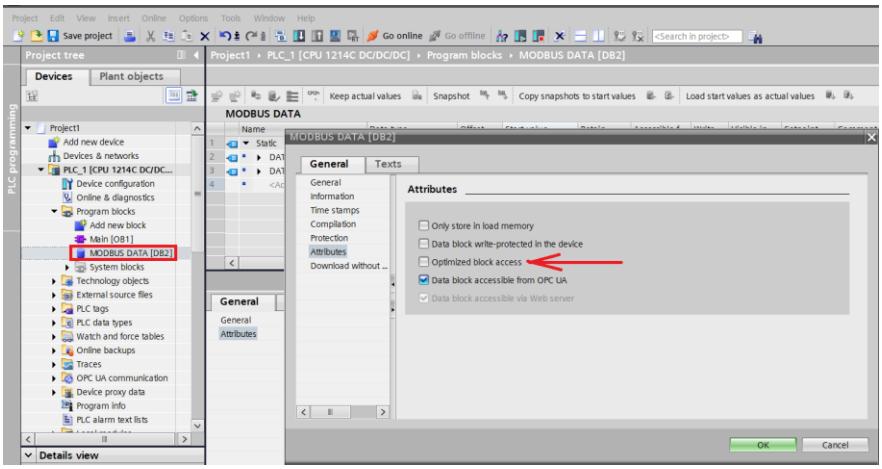

Figura 68. Configurar Modbus Server en TIA Portal 2.

Se crea un nuevo data block con los parámetros de Modbus. Nótese que se ha configurado con el puerto por defecto de Modbus, que es el 502.

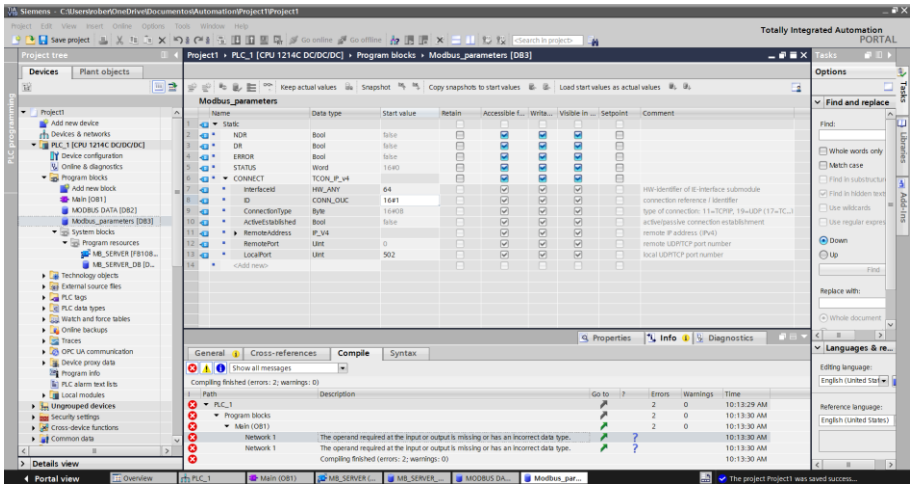

Figura 69. Configurar Modbus Server en TIA Portal 3.

Se accede al área de Program Blocks y Main [OB1].

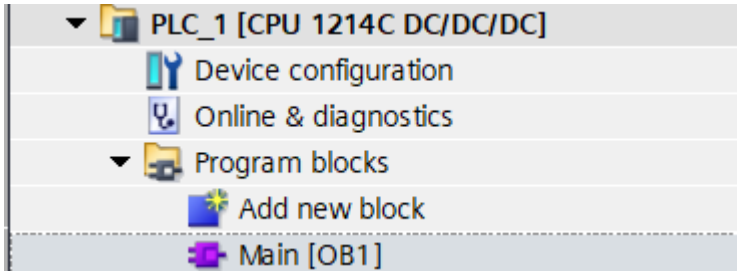

Figura 70. Configurar Modbus Server en TIA Portal 4.

En la pestaña de comunicación, se selecciona MODBUS TCP > MB_SERVER.

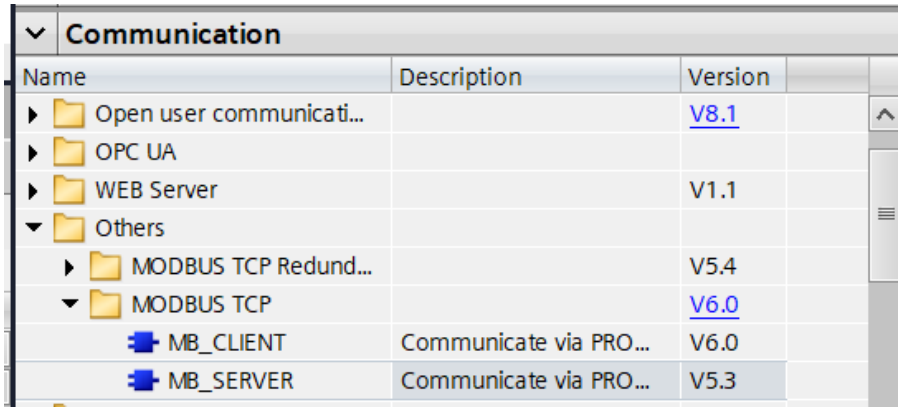

Figura 71. Configurar Modbus Server en TIA Portal 5.

Arrastramos el bloque hasta la ventana principal, y presionamos “Ok”.

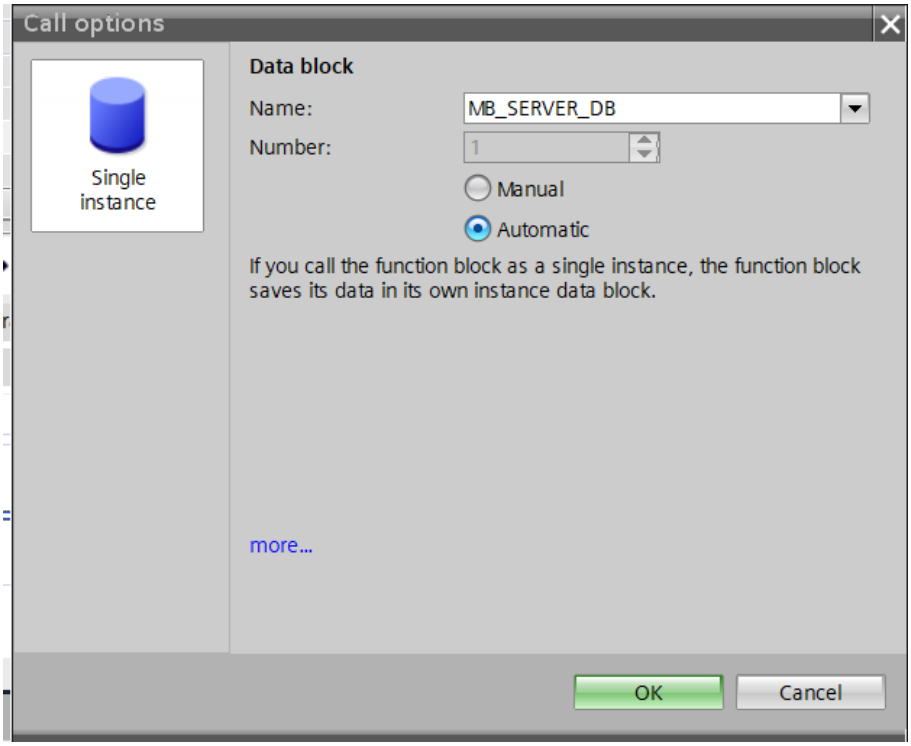

Figura 72. Configurar Modbus Server en TIA Portal 6.

Finalmente se configura el bloque Modbus con los parámetros que se han creado específicamente para ello.

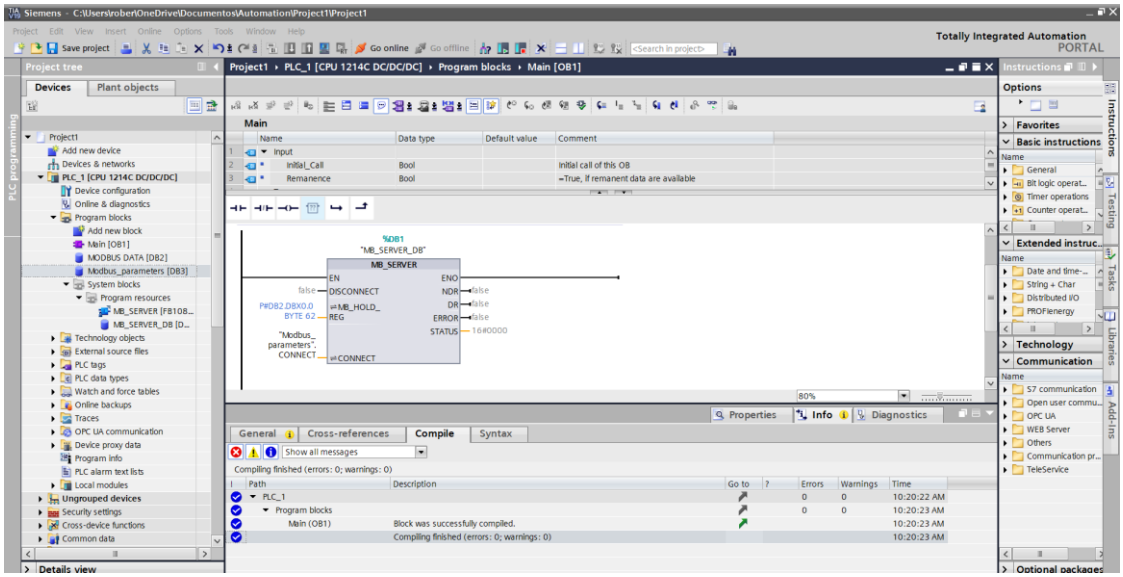

Figura 73. Configurar Modbus Server en TIA Portal 7.

Se abre el programa PLCSIM Advanced v3.0, se selecciona “Start Virtual S7-1500” y se configura con la IP establecida en el dispositivo.

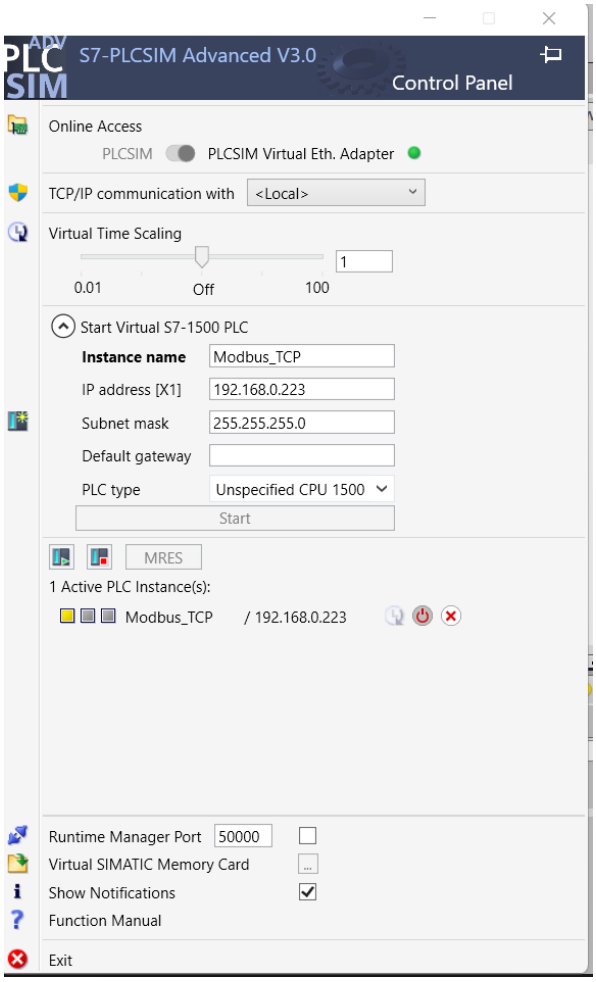

Figura 74. Configurar Modbus Server en TIA Portal 8.

En las propiedades del proyecto, habilita la opción de compilación mediante se ejecuta la simulación del PLC.

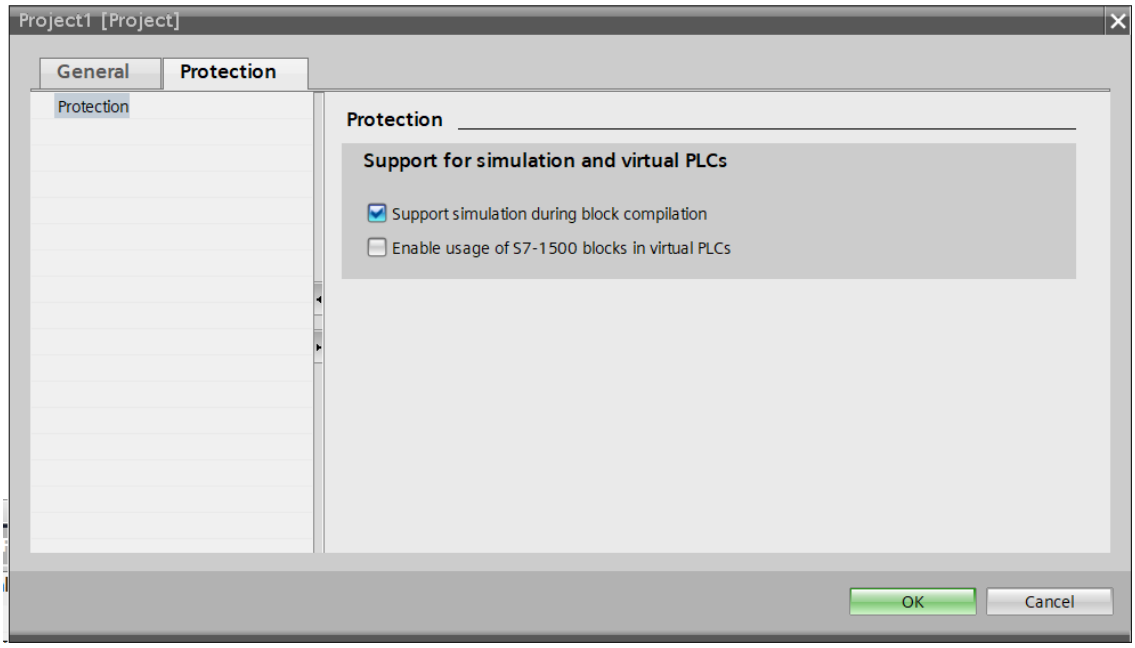

Figura 75. Configurar Modbus Server en TIA Portal 9.

I.2. PLCInjector

Se ha desargado del repositorio de github en Kali Linux mediante el comando:

```
git clone https://github.com/BorjaMerino/PlcInjector.git
```

A continuación, se puede ejecutar la carga de configuración en el PLC mediante:

```
python2 plcInjectPayload.py -upload fichero-malicioso -ip 192.168.0.222
```

Finalmente, se puede descargar la configuración de un PLC, en este ejemplo, se toma que el fichero tiene 1536 bytes.

```
python2 plcInjectPayload.py -download 1536 -ip 192.168.0.222
```

I.3. Docker compose

El fichero docker-compose.yml contiene los servicios de logstash, elasticsearch, kibana, thehive y snort (2 y 3).

```
version: '3.8'

services:
  snort3:
    container_name: snort3
    image: oliwave/snort3:latest
    tty: true
    volumes:
      - ./snort/etc/:/etc/snort/
      - ./snort/log:/var/log/snort
      - ../pcaps:/opt/pcap
    networks:
      - elk
    entrypoint: ["/bin/sh"]

  snort2:
    container_name: snort2
    image: opennsm/snort:2.9.8.0 #ciscotalos/snort3:latest
    tty: true
    volumes:
      - ./snort2/etc/:/etc/snort/
      - ./snort2/log:/var/log/snort
      - ../pcaps:/opt/pcap
    networks:
      - elk
    entrypoint: ["/bin/sh"]

  logstash:
    container_name: logstash
    image: docker.elastic.co/logstash/logstash:7.11.1
    restart: unless-stopped
    networks:
      - elk
    ports:
      - "12201:12201/udp"
      - "5044:5044"
```

```
      - “5000:5000/tcp”
      - “5000:5000/udp”
      - “9600:9600”
    volumes:
      # Fichero de configuración de la aplicación completa.
      - ./logstash/config/pipelines.yml:/usr/share/logstash/config/pipelines.yml

      # Directorio en el que se encuentran los ficheros de configuración de los correspondientes pipelines (flujos de datos entrantes).
      - ./logstash/pipeline:/usr/share/logstash/pipeline

      # Ficheros de logs que logstash va a leer
      - ./logstash/logs/syslog:/usr/share/logstash/data/syslog

      # Ficheros de log de snort
      - ./snort/log:/var/log/snort
      - ./snort2/log:/var/log/snort2

    logging:
      driver: gelf
      options:
        gelf-address: udp://localhost:12201
        tag: logstash

  elasticsearch:
    container_name: elasticsearch
    image: docker.elastic.co/elasticsearch/elasticsearch:7.11.1 #8.10.2 #5.6.0
    restart: unless-stopped
    networks:
      - elk
    ports:
      - 9200:9200
      - 9300:9300
    environment:
      - http.host=0.0.0.0
      - discovery.type=single-node
      - cluster.name=hive
      - script.allowed_types= inline
      - thread_pool.search.queue_size=100000
      - thread_pool.write.queue_size=10000
      - gateway.recover_after_nodes=1
```

```
      - xpack.security.enabled=false
      - bootstrap.memory_lock=true
      - "ES_JAVA_OPTS=-Xms512m -Xmx512m"
      - transport.host=0.0.0.0
    ulimits:
      nofile:
        soft: 65536
        hard: 65536
    logging:
      driver: gelf
      options:
        gelf-address: udp://localhost:12201
        tag: elasticsearch

  kibana:
    container_name: kibana
    image: docker.elastic.co/kibana/kibana:7.11.1 #8.10.2 #5.6.0
    restart: unless-stopped
    networks:
      - elk
    ports:
      - "5601:5601"
    logging:
      driver: gelf
      options:
        gelf-address: udp://localhost:12201
        tag: kibana

  thehive:
    container_name: thehive
    image: thehiveproject/thehive:3.5.1-1 #latest
    depends_on:
      - elasticsearch
    ports:
      - "0.0.0.0:9000:9000"
    volumes:
        - ./thehive/etc/application.conf:/etc/thehive/application.conf
    command:
      --no-config-cortex
```

```
      --es-uri http://elasticsearch:9200
    networks:
      - elk

  alert_monitor:
    container_name: alert_monitor
    image: python:3.9.19-bullseye #latest
    depends_on:
      - thehive
      - elasticsearch
    volumes:
        - ./alert_monitor:/opt/alert_monitor
    command:  >
      sh -c “pip install thehive4py &&
             pip install elasticsearch==7.11.0 &&
             python /opt/alert_monitor/create_alerts.py”
    networks:
      - elk

networks:
  elk:
    driver: bridge
```

I.4. Elasticsearch

La configuración de elasticsearch se ha dejado por defecto. Para crear el índice de snort en elasticsearch, se usa la interfaz de kibana, desde la pestaña de Stack Management > Index Management > Templates > Create template.

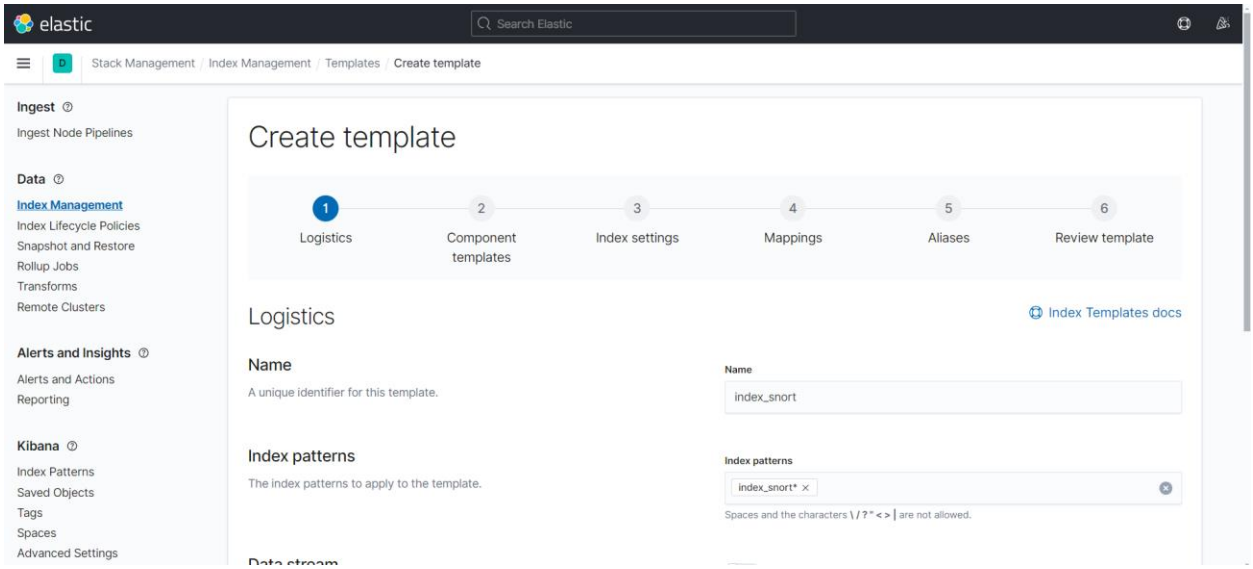

Figura 76. Creación del índice de snort en elasticsearch 1.

Se presiona “Next” hasta llegar a la última pantalla, donde se procede a crear el índice.

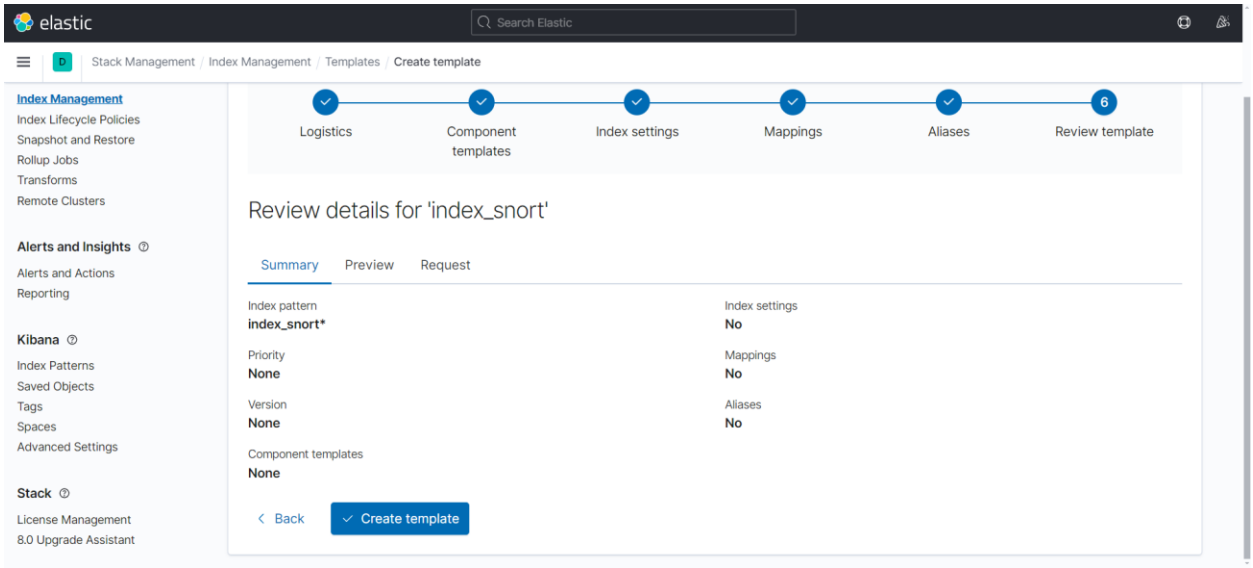

Figura 77. Creación del índice de snort en elasticsearch 2.

A continuación, se accede a la sección “Discover” y se tendrá que crear el index_patern que permita hacer búsquedas sobre el índice que se ha creado.

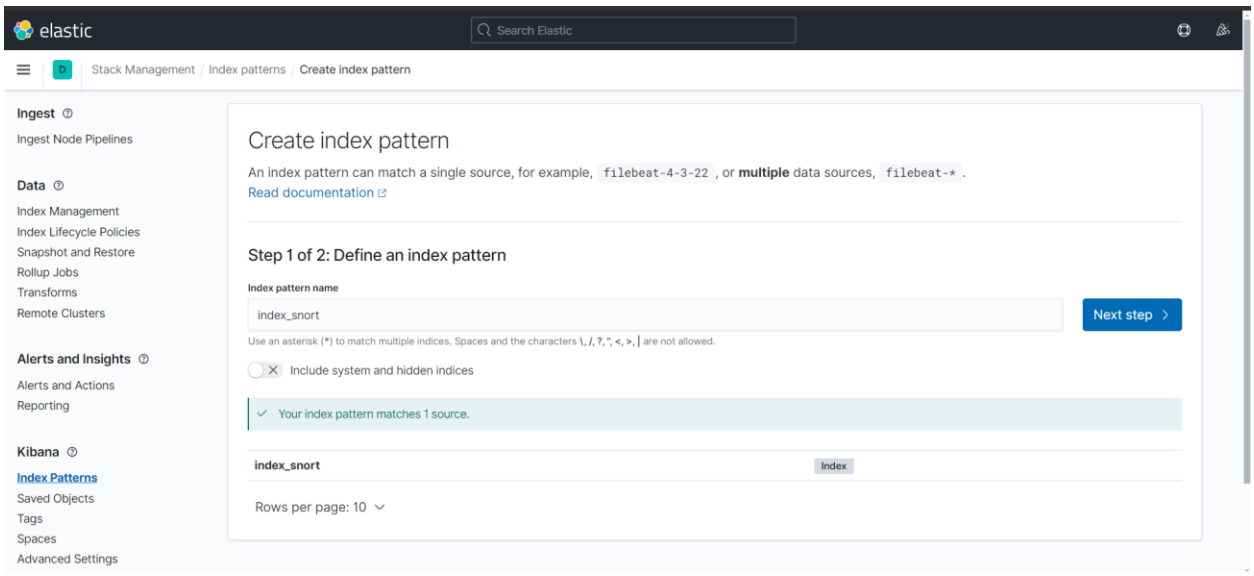

Figura 78. Creación del patrón del índice de snort 1.

Y después se seleccionará el campo que corresponda al timestamp para poder hacer búsquedas temporales.

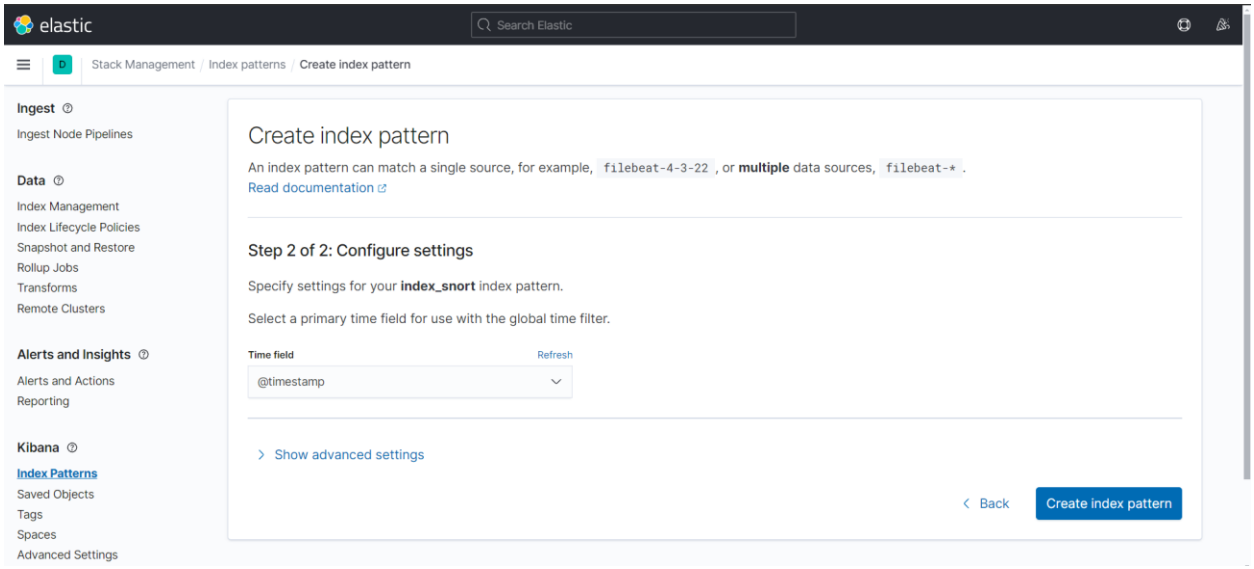

Figura 79. Creación del patrón del índice de snort 2.

Se crea otro índice llamado “index_thehive” para tener monitorizadas las alertas también en la base de datos de elasticsearch.