IMPLEMENTACIÓN DE UNA PRUEBA DE CIBERSEGURIDAD ENFOCADA EN EVALUAR LA VULNERABILIDAD DE LA UNIDAD DE MEDIDA EN SISTEMAS AMI ANTE EL ATAQUE DE DENEGACIÓN DE SERVICIO.

Karold Juliana Muñoz Fernández
karold.munoz@correounivalle.edu.co



Escuela de Ingeniería Eléctrica y Electrónica
Facultad de Ingeniería
Santiago de Cali
Diciembre 2025

IMPLEMENTACIÓN DE UNA PRUEBA DE CIBERSEGURIDAD ENFOCADA EN EVALUAR LA VULNERABILIDAD DE LA UNIDAD DE MEDIDA EN SISTEMAS AMI ANTE EL ATAQUE DE DENEGACIÓN DE SERVICIO.

Karold Juliana Muñoz Fernández
karold.munoz@correounivalle.edu.co

Documento presentado a
Programa de Pregrado en Ingeniería Electrónica - 3744
como requisito para optar por el título de
Ingeniera Electrónica

Directores: Eduardo Francisco Caicedo Bravo, Ph.D.
Profesor Titular - EIEE
Cristian Fernando Rodríguez Cardona, M.Sc.
Líder de Producto - Metrum Soluciones Inteligentes S.A.S



Escuela de Ingeniería Eléctrica y Electrónica
Facultad de Ingeniería
Santiago de Cali
Diciembre 2025

RESUMEN

La modernización del sector eléctrico mediante la implementación de redes inteligentes ha impulsado la adopción de los Sistemas de Medición Avanzada (AMI), los cuales integran tecnologías de comunicación y dispositivos inteligentes que permiten una gestión más eficiente de la energía. Sin embargo, esta digitalización también incrementa la exposición a ciberamenazas, convirtiendo a la unidad de medida en un componente crítico desde el punto de vista de la ciberseguridad. En este contexto, el presente trabajo de grado se enfocó en el análisis del comportamiento de un ataque de denegación de servicio (DoS) aplicado sobre la unidad de medida dentro de un entorno AMI.

El objetivo principal del trabajo fue analizar el comportamiento del ataque DoS con respecto a la variable del consumo de energía eléctrica, a partir de pruebas realizadas en un entorno de laboratorio controlado. Para ello, se desarrolló una metodología que permitió estructurar el proceso necesario para la ejecución de la prueba de vulnerabilidad, considerando las técnicas a usar, los requerimientos, elementos, montajes físicos y el análisis de los resultados obtenidos de la prueba. Este enfoque permitió comprender que la aplicación de técnicas de ciberseguridad no se limita a la ejecución del ataque, sino que requiere un proceso previo de análisis y entendimiento del sistema evaluado.

Los resultados obtenidos permitieron observar el comportamiento del sistema ante la presencia del ataque DoS, aportando información relevante sobre la respuesta de la unidad de medida bajo condiciones de estrés. Si bien el alcance del estudio se limitó a un tipo específico de ataque y a un único componente de la infraestructura AMI, los hallazgos constituyen una base técnica que puede ser utilizada como referencia para futuras evaluaciones de ciberseguridad.

Finalmente, este trabajo contribuye al ámbito académico y técnico al aportar un análisis estructurado del comportamiento de ataques de denegación de servicio en sistemas AMI, resaltando la importancia de fortalecer las evaluaciones de ciberseguridad en la unidad de medida como parte del proceso de evolución hacia redes eléctricas inteligentes más seguras y resilientes.

Palabras clave– Smart Grids, ciberseguridad, sector eléctrico, infraestructura de medición avanzada, denegación de servicio, fuzzing, flooding.

ABSTRACT

The modernization of the electricity sector through the implementation of smart grids has driven the adoption of Advanced Metering Infrastructure (AMI) systems, which integrate communication technologies and smart devices that enable more efficient energy management. However, this digitization also increases exposure to cyber threats, making the metering unit a critical component from a cybersecurity perspective. In this context, this thesis focused on analyzing the behavior of a denial-of-service (DoS) attack applied to the metering unit within an AMI environment.

The main objective of the thesis was to analyze the behavior of the DoS attack with respect to the variable of electricity consumption, based on tests carried out in a controlled laboratory environment. To this end, a methodology was developed that allowed the process necessary for the execution of the vulnerability test to be structured, considering the techniques to be used, the requirements, elements, physical setups, and the analysis of the results obtained from the test. This approach made it possible to understand that the application of cybersecurity techniques is not limited to the execution of the attack, but requires a prior process of analysis and understanding of the system being evaluated.

The results obtained allowed us to observe the behavior of the system in the presence of a DoS attack, providing relevant information about the response of the metering unit under stress conditions. Although the scope of the study was limited to a specific type of attack and a single component of the AMI infrastructure, the findings constitute a technical basis that can be used as a reference for future cybersecurity assessments.

Finally, this work contributes to the academic and technical fields by providing a structured analysis of the behavior of denial-of-service attacks on AMI systems, highlighting the importance of strengthening cybersecurity assessments in the metering unit as part of the process of evolving toward more secure and resilient smart grids.

Keywords– Smart Grids, cybersecurity, electricity sector, advanced metering infrastructure, denial of service, fuzzing, flooding.

DEDICATORIA

En primer lugar, a Dios, por guiar cada uno de mis pasos, darme la fortaleza en los momentos difíciles y permitirme culminar esta etapa tan importante de mi vida.

A mis padres, Luz Denis y Rubén, quienes han sido mi mayor ejemplo de amor, esfuerzo y perseverancia. Gracias por su apoyo incondicional, por creer en mí incluso cuando yo dudaba, por acompañarme en cada etapa de mi vida y por enseñarme valores que hoy me definen como persona. Este logro también es de ustedes.

A mi hermana Katherin, por ser un apoyo constante, por su motivación, su ayuda incondicional y por impulsarme siempre a ser mejor persona. A mi hermano Óscar, por su respaldo y acompañamiento. A mi sobrino Ian, por regalarme sonrisas sinceras, por enseñarme a ver el mundo con otros ojos y por ser una fuente de alegría y fortaleza. A mi perrita Aria, por su compañía incondicional durante los trasnochos, por su alegría silenciosa y por recordarme, incluso en los momentos de mayor cansancio, la importancia de la calma, el cariño y la constancia.

A mi abuela Miriam, que hoy no se encuentra presente, pero cuya preocupación y desvelo por mis trasnochos dedicados a la universidad hoy cobran sentido y frutos. Su amor, cuidado y palabras siguen acompañándome y siendo una guía constante en mi vida.

A mi pareja Robinson, por su amor, paciencia y perseverancia. Gracias por estar a mi lado durante todo este proceso, por motivarme cuando las fuerzas faltaban, por ayudarme a superar cada obstáculo y por convertirse en un pilar fundamental en este camino.

Finalmente, dedico este trabajo de grado al desarrollo de las redes eléctricas inteligentes, como símbolo del avance tecnológico y de la transformación del sector energético hacia sistemas más eficientes, sostenibles y seguros. A quienes trabajan día a día por fortalecer la ciberseguridad, no solo como una disciplina técnica, sino como un compromiso con la protección de infraestructuras críticas. Este trabajo representa un pequeño aporte al camino que recorremos quienes creemos en un desarrollo tecnológico responsable, seguro y con sentido humano.

A los jóvenes que, como yo, creen en la ingeniería, la investigación y la innovación como motores para construir un mejor futuro y aportar soluciones a los desafíos tecnológicos de nuestra sociedad.

AGRADECIMIENTOS

A mis directores de trabajo de grado, Eduardo Caicedo y Cristian Rodríguez, por la confianza depositada en mí, su dedicación, paciencia y constante disposición durante el desarrollo de este trabajo de grado, el cual representó un gran reto académico y personal. Su acompañamiento, orientación y apoyo fueron fundamentales para alcanzar los objetivos propuestos. Agradezco profundamente su profesionalismo, experiencia y compromiso con mi formación académica y personal. Ha sido un honor trabajar junto a ustedes y aprender de su ejemplo.

A Bayron Calvache, por sus valiosos consejos y recomendaciones, que fueron fundamentales para superar barreras de conocimiento y avanzar con mayor claridad hacia el cumplimiento de los objetivos planteados. Agradezco su disposición, dedicación y paciencia para guiarme en el camino correcto, así como por compartir su conocimiento y darme a conocer el amplio y apasionante mundo de las redes eléctricas inteligentes.

A mis amigos y compañeros Joshua Arango y Daniel Valderrama, con quienes tuve el privilegio de conformar un grupo académico desde los primeros semestres. Gracias por acompañarme durante esta etapa académica y formativa, por las experiencias compartidas y por el apoyo mutuo que hizo de este proceso un camino más llevadero y enriquecedor. A Alexis Murillo, Alejandro Escobar y Carla Juliana, compañeros y amigos que encontré a lo largo del camino. Junto a ustedes construimos una relación basada en la amistad, el compromiso y la colaboración, que permitió transformar cada reto académico en una oportunidad de aprendizaje. Más allá de lo académico, compartimos experiencias únicas, momentos de calidez, autenticidad, risas y vivencias que enriquecieron profundamente esta etapa de mi vida.

Finalmente, culminar esta etapa representa mucho más que alcanzar una meta académica. Mi paso por la universidad no solo me permitió adquirir conocimientos, sino también crecer como persona, superar desafíos y rodearme de personas maravillosas que dejaron una huella imborrable en mi vida.

Siglas

AMI Advanced Metering Infraestructure. 1–4, 7, 16–23, 25–30, 32–40, 43, 48, 56

APT Amenaza Persistente Avanzada. 15

CCI Centro de Ciberseguridad Industrial. 2

CIA Confidentiality, Integrity y Availability. 1, 3, 13, 14

CIM Common Information Model. 8, 11

CNO Consejo Nacional de Operación. 12, 13

DCU Unidad de Concentracón de Datos. 25, 30

DDoS Denegación de Servicio Distribuida. 15, 25, 26, 28–30

DER Distributed Energy Resources. 11, 34, 35

DLMS/COSEM Device Language Message Specification/Companion Specification for Energy Metering. 32, 33, 39–47, 57

DoS Denegación de servicios. 1–4, 15, 17, 18, 25–30, 32, 39

EPRI Electric Power Research Institute. 6, 11

ETIP SNET European Technology and Innovation Platforms Smart Networks for Energy Transition. 20

GWAC GridWise Architecture Council. 10

HAN Red de Área Domestica. 25, 26

HES Head End System. 16, 19, 35, 38, 39, 42

IEC International Electrotechnical Commission. 8, 11, 41

IED Intelligent Electronic Device. 11

IIoT Industrial Internet of Things. 7, 11

IoT Internet de las Cosas. 17, 26, 30

IT Tecnologías de la Información. 8, 11, 12

JRC Joint Research Centre. 19, 20, 24

MDM Gestión de datos de medición. 35

NAN Red de Área de Vecindario. 25, 26

NCCoE National Cybersecurity Center of Excellence. 1

NIST Instituto Nacional de Estándares y Tecnología de Estados Unidos. 2, 5, 7, 8

OBIS Sistema de Identificación de Objetos. 33, 41, 43, 44, 57, 58

OpenADR Open Automated Demand Response. 24

OSI Open Systems Interconnection. 32, 33

OT Tecnologías de la Operación. 8, 11, 12

PLC Power Line Communications. 22, 23

PMU Phasor Measurement Unit. 7

REI Red Eléctrica Inteligente. 1, 2, 5, 6, 9, 11, 36

RTU Remote Terminal Unit. 7

SCADA Sistemas de Control y Adquisición de Datos. 2, 12

SEP Sistema Eléctrico de Potencia. 8, 27

SG Smart Grid. 1, 6–8, 11, 13, 15, 19, 20, 27, 28

SGO Sistema de Gestión y Operación. 35

SIN Sistema Interconectado Nacional. 13

TIC Tecnologías de la Información y la Comunicación. 6

TO Tecnologías de la Operación. 6

UC Unidad Concentradora. 35, 39

UM Unidad de Medida. 4, 16, 34, 35

WAN Red de Área Amplia. 25, 26

WLAN Red de Área Local Inalámbrica. 29

TABLA DE CONTENIDO

Pag.

RESUMEN ..... **I**

ABSTRACT ..... **II**

DEDICATORIA ..... **III**

AGRADECIMIENTOS ..... **IV**

TABLA DE CONTENIDO ..... **VII**

ÍNDICE DE FIGURAS ..... **X**

ÍNDICE DE TABLAS ..... **XII**

1. INTRODUCCIÓN **1**

1.1. Contexto 2
1.2. Objetivos 3
1.2.1. Objetivo General 3
1.2.2. Objetivos Específicos 3
1.3. Estructura del Documento 4
1.4. Principales Aportes y Resultados Obtenidos 4

2. ANTECEDENTES Y NORMATIVAS **5**

2.1. Introducción 5
2.2. Redes Eléctricas Inteligentes 5
2.2.1. Aspectos clave de las REI 6
2.2.2. Modelo Conceptual e Interoperabilidad 7
2.2.2.1. Modelo Conceptual del CIM 8
2.2.2.2. Modelo de Interoperabilidad del NIST 8
2.2.2.3. Interacción Entre Dominios 9
2.2.2.4. Interacción Entre Capas 10
2.3. Ciberseguridad en Smart Grids y AMI 11
2.3.1. Ciberseguridad en el Contexto de la Evolución de las Redes Eléctricas 11
2.3.1.1. Estándares de Ciberseguridad en el Sector Eléctrico 12
2.3.1.2. Estándares de Ciberseguridad en el Sector Eléctrico Colombiano ... 12
2.3.1.3. Digitalización de la Energía: Un Nuevo Paradigma de Ciberseguridad 13
2.3.2. Revisión Bibliométrica Sobre Ciberseguridad en la Unidad de Medida 16
2.3.2.1. Revisión Bibliométrica General sobre Ciberseguridad y Ciberataques 17
2.3.2.2. Identificación Bibliométrica de Técnicas Asociadas a Ataques DoS . 18
2.4. Laboratorios de Sistemas AMI 19

2.4.1. Revisión de Laboratorios de Smart Grid y AMI 19
2.4.2. Normas Técnicas Bajo las Cuales Están Acreditados los Laboratorios 21
2.4.2.1. Respuesta de la Demanda 24
2.5. Laboratorios de Ciberseguridad: Análisis de DoS en AMI 25
2.5.1. Equipos y Hardware Utilizados 25
2.5.2. Software de Simulación y Emulación para el Análisis de DoS/DDoS 25
2.5.3. Normativas de Protocolos Relevantes en AMI 26
2.5.4. Protocolos de Enrutamiento 27
2.5.5. Ataque de Denegación de Servicio DoS 27
2.5.5.1. La Amenaza de Ataques de DoS en AMI 28
2.5.5.2. Mecanismos de Ataque DoS/DDoS en Sistemas AMI 29
2.5.5.3. Consecuencia de un Ataque DoS/DDoS en Sistemas AMI 30
2.6. Síntesis 31

3. METODOLOGÍA PARA UNA PRUEBA DE VULNERABILIDAD 32

3.1. Introducción 32
3.1.1. Infraestructura de Medición Avanzada (AMI) en el contexto del modelo OSI 32
3.2. AMI (Advance Metering Infraestructure) 34
3.2.1. Unidad de Medida (UM) 34
3.2.2. Sistema de Gestión y Operación (SGO) o Head End System (HES) 35
3.2.3. Unidad Concentradora (UC) 35
3.2.4. Comunicaciones 35
3.2.5. Seguridad 36
3.3. Medidor inteligente (Smart Meter) 36
3.3.1. Componentes principales del medidor inteligente 37
3.4. Plataformas de unidad de medida basadas en DLMS/COSEM 39
3.4.1. Características técnicas de los protocolos PLC utilizados 40
3.5. Protocolo DLMS/COSEM 40
3.5.1. Estructura y documentación del protocolo DLMS/COSEM 42
3.5.2. Sistema de Identificación OBIS 43
3.5.3. Seguridad, autenticación y control de acceso en DLMS/COSEM 44
3.6. Vulnerabilidades del protocolo DLMS/COSEM 46
3.6.1. Vulnerabilidades inherentes al protocolo 46
3.6.2. Vulnerabilidades de implementación (errores operativos y de desarrollo) 47
3.7. Técnicas para la implementación de las pruebas 48
3.8. Técnicas aplicadas para la implementación de las pruebas en el medidor STAR 49
3.8.1. Opción 1: Fuzzing con perfil de escritura adaptado a DLMS/COSEM 49
3.8.1.1. Inicialización de sesión y perfil de comunicación 49
3.8.1.2. Objeto y control sintáctico mínimo 49
3.8.1.3. Generación de *payloads* y ejecución indefinida 49
3.8.2. Flujo de ejecución del script de fuzzing 50
3.8.3. Opción 2: Flooding de lectura (stress) con perfil de lectura 51
3.8.3.1. Arquitectura del script 51
3.8.3.2. Flujo de ejecución del flooding de lectura 52
3.8.4. Opción 3: Flooding de lectura en perfil (sin autenticación) 53
3.8.4.1. Arquitectura del script 53

3.8.4.2. Flujo de ejecución del flooding en perfil 54
3.9. Requerimientos para la prueba de DoS 55
3.9.1. Elementos para la prueba de DoS 55
3.9.1.1. Equipo computacional como servidor y generador de tráfico 55
3.9.1.2. Especificaciones técnicas del equipo 55
3.9.1.3. Medidor Inteligente DTS27 de Star Instrument 56
3.9.1.4. GuruX 57
3.10. Síntesis 58

4. DISPOSICIÓN FUNCIONAL Y RESULTADO DE LA PRUEBA 59

4.1. Introducción 59
4.2. Montaje de la prueba 59
4.2.1. Medidor vulnerables y medidor de referencia 59
4.2.2. Carga Fantasma Trifásica 3F 61
4.2.3. Consumo de energía eléctrica como variable crítica de operación y facturación 62
4.2.4. Tipo de ataque evaluado 63
4.2.5. Introducción a la obtención y análisis de los resultados 63
4.2.6. Análisis del comportamiento del medidor bajo condiciones de estrés. 64
4.2.6.1. Comportamiento del medidor en condición sin estrés 64
4.2.6.2. Comportamiento del medidor bajo condición de estrés 65
4.2.6.3. Prueba 1: Fuzzing en el perfil de escrtiura 65
4.2.6.4. Prueba 2: Flooding en el perfil de lectura 67
4.2.6.5. Prueba 3: Flooding en el perfil publico 68
4.3. Evaluación de la Susceptibilidad frente a Ataques DoS 70
4.3.1. Definición de Métricas Cuantitativas para la Evaluación de Ataques DoS 70
4.3.1.1. Tasa de Error de Disponibilidad (DER) 71
4.3.1.2. Índice de Latencia Acumulada (ALI / RTT) 71
4.3.2. Análisis de la susceptibilidad de las pruebas de DoS 71
4.4. Discusión 73

5. CONCLUSIONES Y TRABAJOS FUTUROS 74

5.1. Conclusiones Generales 74
5.2. Trabajos Futuros 75

REFERENCIAS 76

ÍNDICE DE FIGURAS

FIGURA Pag.

2.1. Smart Grid en el sector TIC. 6

2.2. Arquitectura basada en el modelo CIM. 7

2.3. Modelo Conceptual y dominios de la Smart Grid (SG). 9

2.4. Modelo arquitectural SGAM. 10

2.5. Objetivos y requerimientos de la ciberseguridad en Smart Grid. 14

2.6. Requerimiento de la CIA en terminos de ciberseguridad. 14

2.7. Secuencia de un ciberataque. 15

2.8. Bibliometría orientada a ciberseguridad. 17

2.9. Bibliometría orientada a ciberseguridad (DoS) 17

2.10. Laboratorios por el continente de Europa, América, Oceanía y África. 20

2.11. Áreas de investigación de AMI y porcentaje de laboratorios. 21

2.12. Normas y tecnologías aplicadas para laboratorios AMI. 23

3.1. Modelo OSI 33

3.2. Arquitectura del sistema AMI. 34

3.3. Componentes del medidor inteligente 39

3.4. Plataformas de unidad de medida 40

4.1. Diagrama metodológico del montaje de la prueba. 61

4.2. Comportamiento del medidor sin estrés 65

4.3. Comportamiento del medidor con estrés - Prueba fuzzing perfil escritura 24 horas... 66

4.4. Comportamiento del medidor con estrés-Prueba fuzzing-escritura con escalonamiento. 67

4.5. Comportamiento del medidor con estrés-Prueba flooding lectura con escalonamiento 67

4.6. Comportamiento del medidor con estrés - Prueba flooding perfil lectura 24 horas ... 68

4.7. Comportamiento del medidor con estrés - Prueba flooding perfil público 24 horas ... 69

4.8. Comportamiento del medidor con estrés - Prueba flooding perfil público con escalonamiento 69

5.1. Diagrama general para realizar una prueba de vulnerabilidad en medidores AMI. ... 82

5.2. Diagrama para realizar una prueba de vulnerabilidad en medidores AMI, secciones I - A, A - B1, B1 - B2, B2 - C, C - F..... 83

ÍNDICE DE TABLAS

TABLA Pag.

2.1. Estándares IEC para Smart Grids 8

2.2. Dominios del Modelo Conceptual de Smart Grids 9

2.3. Capas del Modelo Conceptual de Smart Grid 11

2.4. Estándares de ciberseguridad en el sector eléctrico 12

2.5. Resultados de la ecuación de búsqueda específica de ciberseguridad en sistemas AMI. 16

2.6. Resultados de la ecuación de búsqueda general en ciberseguridad y ciberataques. ... 18

2.7. Normas acreditadas por laboratorios 22

2.8. Estándares aplicados para los laboratorios 22

2.9. Normas utilizadas por los laboratorios 24

2.10. Normas y laboratorios en AMI 24

2.11. Software de simulación y emulación para el análisis de DoS/DDoS en AMI 26

3.1. Fichas técnicas de las plataformas de unidad de medida basadas en DLMS/COSEM. 41

3.2. Descripción de los campos del código OBIS 43

3.3. Valores del campo A del código OBIS 44

3.4. Clasificación de las familias de estímulos de fuzzing aplicadas sobre el objeto COSEM seleccionado, manteniendo coherencia sintáctica con el tipo de dato configurado. 51

3.5. Clasificación de familias de estímulos para flooding de lectura sobre el perfil de carga. 53

3.6. Familias de estímulos definidas para flooding de lectura en perfil 54

4.1. Comparativa de resultados de las pruebas de DoS en la unidad de medida 72

1. INTRODUCCIÓN

El avance tecnológico y la digitalización del sector eléctrico han propiciado una transformación en la gestión y distribución de la energía. En los últimos años, se ha producido un cambio en la concepción y operación de las redes eléctricas, orientado hacia la implementación de redes eléctricas inteligentes que integran tecnologías de información y comunicación para mejorar la interoperabilidad, la eficiencia, la confiabilidad y la seguridad del sistema eléctrico [1]. En respuesta a estos desafíos, ha surgido el concepto de *Red Eléctrica Inteligente (REI)* o *Smart Grid (SG)*, que busca adaptar las redes de próxima generación para gestionar tanto el flujo de datos como de energía de manera eficiente [2].

Como parte de esta evolución, los *Advanced Metering Infraestructure (AMI)* se han convertido en una pieza clave para gestionar de manera eficiente el consumo y la distribución de energía, gracias a su capacidad para recopilar datos en tiempo real y gestionar medidores de forma remota. Sin embargo, este avance tecnológico incrementa los riesgos de ciberseguridad, lo que hace indispensable contar con laboratorios especializados y equipados para garantizar la seguridad de estos sistemas. Estos laboratorios deben ser capaces de someter los medidores a pruebas que garanticen que no sean vulnerables ante ataques cibernéticos, cumpliendo con los controles necesarios para preservar la *Confidentiality, Integrity y Availability (CIA)* de los sistemas de comunicación, control, operación y gestión de la red eléctrica. Asegurar estos principios es fundamental para garantizar la integridad operativa y la continuidad de los servicios de la empresa [3].

A nivel internacional, el *National Cybersecurity Center of Excellence (NCCoE)* en Estados Unidos se destaca por colaborar con la industria para desarrollar soluciones de ciberseguridad para sistemas *AMI*, utilizando entornos simulados avanzados para replicar escenarios de ataques reales. Estos entornos permiten identificar vulnerabilidades en los sistemas de medición avanzada mediante pruebas controladas de ciberataques y mitigar amenazas como ataques de *Denegación de servicios (DoS)* y manipulación de datos [2]. Entre estas amenazas, la *DoS* es una de las más críticas, ya que un cibercriminal puede saturar la red de comunicación de los dispositivos *AMI* con un volumen masivo de solicitudes o tráfico malicioso, esto provoca que los sistemas se vuelvan lentos, no respondan o incluso dejen de funcionar, interrumpiendo la recopilación de datos en tiempo real y la gestión remota de los medidores. Esta vulnerabilidad no solo pone en riesgo la operación continua de las redes eléctricas, sino que también afecta la confianza en la infraestructura, limitando la competitividad de la industria eléctrica y obstaculizando la adopción de tecnologías clave para la transición energética. Además, el *NCCoE* emplea técnicas de monitoreo en tiempo real y evalúa la respuesta de los sistemas *AMI* para poder desarrollar estrategias de mitigación,

como la implementación de controles de acceso, cifrado robusto y procedimientos de respuesta ante incidentes [4]. Un caso representativo de ciberataque en redes eléctricas ocurrió en Ucrania en 2016, cuando el malware CrashOverride interrumpió la operación de varias subestaciones eléctricas mediante la manipulación de los *Sistemas de Control y Adquisición de Datos (SCADA)*, dejando sin electricidad a cientos de miles de usuarios por varias horas. Este ataque fue uno de los primeros casos documentados de interrupción de redes eléctricas mediante un ciberataque dirigido a sistemas de control industrial [5]. Por otro lado, un ejemplo relevante de vulnerabilidad en sistemas *AMI* se registró en Malta entre 2011 y 2012, cuando más de 1.000 medidores inteligentes fueron hackeados para manipular el registro de consumo, permitiendo el robo de electricidad valorado en 30 millones de euros. Los atacantes lograron explotar vulnerabilidades en la comunicación entre los medidores y el sistema de gestión, alterando los registros de facturación y afectando la integridad de los datos transmitidos [6].

En América Latina, un ejemplo relevante es el *Centro de Ciberseguridad Industrial (CCI)* en México y Argentina, que se enfoca en la investigación y el desarrollo de prácticas de seguridad para infraestructuras críticas, incluyendo los *AMI*, mediante la simulación de ataques y la evaluación de vulnerabilidades [3]. Debido a la modernización del sector eléctrico y a la adopción de sistemas *AMI*, surge la necesidad de analizar la exposición de las unidades de medida a amenazas de ciberseguridad. En este contexto, la presente investigación se orienta a la revisión de normativas, lineamientos técnicos y laboratorio asociadas a sistemas *AMI*, y definir los requisitos necesarios para la ejecución de pruebas de vulnerabilidad por *DoS* utilizando los recursos disponibles en el laboratorio de inteligencia computacional de la Universidad del Valle.

1.1 Contexto

En Colombia, la modernización del sector eléctrico ha impulsado la implementación de *AMI* como parte de la evolución hacia las *REI*. Los sistemas *AMI* permiten la recopilación de datos en tiempo real y la gestión remota de medidores. Sin embargo, esta transformación ha traído nuevos desafíos de ciberseguridad, ya que los sistemas *AMI* son vulnerables a ataques que podrían comprometer la continuidad y confiabilidad del servicio eléctrico. Para abordar estos riesgos, es crucial implementar marcos normativos que aseguren la protección y correcta operación. En Colombia, la NTC 6079:2021 establece directrices para la operación segura y eficiente, asegurando que los sistemas cuenten con comunicación bidireccional que permita la conexión y desconexión remota de los medidores manteniendo la integridad de los datos y la seguridad del sistema [7].

En términos de protección, el Framework de Ciberseguridad del *Instituto Nacional de Estándares y Tecnología de Estados Unidos (NIST)* ofrece un enfoque estandarizado para la

protección de infraestructuras críticas como la *AMI*. Este marco se basa en tres pilares fundamentales de la *CIA* [8]. Estos principios aseguran que los sistemas y datos gestionados estén protegidos contra accesos no autorizados, modificaciones maliciosas y fallos que comprometan su disponibilidad. Este proporciona lineamientos para mitigar los riesgos de ciberataques y asegurar la continuidad operativa del sistema, permitiendo alinearse con las mejores pruebas internacionales, garantizando que los procedimientos de prueba y las estrategias de defensa se desarrollen bajo estándares reconocidos globalmente. Además, la ciberseguridad se convierte en un aspecto clave. Dado que estos sistemas se apoyan en la transmisión constante de datos entre los medidores y los sistemas de control, son vulnerables a ataques cibernéticos que buscan comprometer su integridad o disponibilidad. Un estudio de Kumar [9]. sobre la resiliencia de los medidores inteligentes frente a ciberataques subraya la importancia de desarrollar estrategias de defensa robustas para proteger el sistema contra amenazas como el puppet attack, un ataque en el que los nodos de la red *AMI* son explotados para generar tráfico excesivo que congestiona la red, causando una *DoS*. Esto destaca la importancia de diseñar procedimientos experimentales para evaluar la resistencia de los medidores inteligentes. La relevancia se centra en que se definan protocolos precisos para evaluar y mejorar la resiliencia del sistema *AMI* ante ataques específicos.

El safety dentro de *AMI* es otro aspecto que debe ser considerado. Las medidas buscan prevenir cualquier daño físico a las personas, los equipos y el medio ambiente destacan la necesidad de implementar sistemas de protección física, como dispositivos de puesta a tierra y sistemas contra incendios, que aseguren que cualquier fallo tecnológico no afecte la seguridad operativa ni ponga en riesgo a los operarios o al entorno [10]. Al final, la expansión del sistema *AMI* representa un paso clave hacia la modernización y eficiencia de las redes eléctricas en Colombia. Sin embargo, su éxito depende de la implementación de protocolos de ciberseguridad sólidos y de la capacidad para enfrentar amenazas emergentes, asegurando así la confiabilidad y seguridad de las infraestructuras eléctricas en el país.

1.2 Objetivos

1.2.1 Objetivo General

- Implementar una prueba de ciberseguridad en el laboratorio de inteligencia computacional de la Universidad del Valle, enfocada en evaluar la vulnerabilidad de la unidad de medida en sistemas *AMI* ante un ataque de denegación de servicio.

1.2.2 Objetivos Específicos

- Compendiar sistemáticamente las normativas y equipos empleados en laboratorios de ciberseguridad en la unidad de medida para sistemas *AMI*, centrándose en la amenaza ante el ataque de denegación de servicio.

- Definir los requisitos necesarios para realizar la prueba de vulnerabilidad en la unidad de medida en ataques de denegación de servicio en el laboratorio de inteligencia computacional de la Universidad del Valle en donde se encuentran los módulos *AMI*
- Implementar una prueba de vulnerabilidad en la unidad de medida en sistemas *AMI* ante el ataque de denegación de servicio *DoS*, siguiendo los requisitos previamente establecidos.
- Validar los resultados del sistema *AMI* frente a un ataque de denegación de servicio, determinando su grado de susceptibilidad.

1.3 Estructura del Documento

El presente trabajo de grado se organiza en cinco capítulos, estructurados de manera progresiva para abordar el problema de investigación desde el contexto conceptual hasta la validación. El **Capítulo 1** presenta la introducción y el contexto general de la investigación, enmarcando la evolución de las *REI* y los sistemas *AMI*, así como los principales retos de ciberseguridad. En este capítulo se formulan el objetivo general y los objetivos específicos que orientan el desarrollo del estudio. El **Capítulo 2** desarrolla una investigación sistemática sobre normativas, lineamientos técnicos y laboratorios relacionados con la ciberseguridad en sistemas *AMI*, con énfasis en ataques *DoS*. Este capítulo da cumplimiento al primer objetivo específico mediante la revisión de marcos regulatorios y enfoques metodológicos relevantes. El **Capítulo 3** aborda la definición de los requisitos necesarios para la ejecución de la prueba de vulnerabilidad, apoyándose en el diagrama metodológico propuesto. En este capítulo se describen los elementos de la prueba, las técnicas seleccionadas y las restricciones del entorno de laboratorio, dando cumplimiento al segundo objetivo específico. El **Capítulo 4** presenta la implementación de la prueba de vulnerabilidad DoS. Se describen el montaje experimental, los procedimientos aplicados y las técnicas de ataque seleccionadas, en concordancia con los requisitos previamente establecidos. Se realiza el análisis y validación de los resultados obtenidos durante la prueba, permitiendo determinar el grado de susceptibilidad de la *Unidad de Medida (UM)* bajo prueba frente a ataques *DoS*.

1.4 Principales Aportes y Resultados Obtenidos

Este trabajo de grado aportó al estudio de la ciberseguridad en sistemas de medición avanzada (AMI), analizando el comportamiento de un ataque de denegación de servicio sobre la unidad de medida en relación con la variable de consumo de energía eléctrica. A través de pruebas realizadas en un entorno de laboratorio, se analizó la respuesta del sistema ante este tipo de ataque, permitiendo identificar su comportamiento bajo condiciones controladas. Los resultados obtenidos constituyen un insumo técnico que puede servir como referencia para el desarrollo de futuras evaluaciones de ciberseguridad en sistemas AMI y para la ampliación del análisis hacia otros escenarios y tipos de ataque.

2. ANTECEDENTES Y NORMATIVAS

2.1 Introducción

Este capítulo desarrolla una revisión sistemática de los fundamentos conceptuales, normativos y técnicos asociados a los sistemas de medición avanzada (*AMI*) y su relación con la ciberseguridad en el sector eléctrico. El análisis se orienta a consolidar investigación necesaria para comprender el contexto en el que operan los medidores inteligentes, así como las amenazas que afectan su disponibilidad, con énfasis en ataques de denegación de servicio (*DoS*).

En primer lugar, se abordan los conceptos de *Smart Grid* y *Red Eléctrica Inteligente*, los cuales, para efectos de este trabajo de grado, se consideran equivalentes y se emplean indistintamente para referirse al mismo concepto. Asimismo, se abordar conceptos de sistemas *AMI*, destacando los modelos de interoperabilidad, la interacción entre dominios y los marcos de referencia ampliamente aceptados, como los propuestos por el *NIST*. Posteriormente, se analiza la ciberseguridad aplicada a infraestructuras eléctricas inteligentes, incluyendo estándares internacionales, lineamientos adoptados en el contexto colombiano y la digitalización del sector energético.

Finalmente, se revisan los laboratorios de sistemas *AMI* y ciberseguridad orientados a *AMI*, los equipos y herramientas utilizados, las normativas que los regulan y los tipos de pruebas asociadas a ataques *DoS* y *DDoS*. Esta revisión permite establecer un marco teórico y normativo que sustenta la definición de requisitos y el diseño experimental desarrollados en los capítulos posteriores.

2.2 Redes Eléctricas Inteligentes

Diversas instituciones han definido el concepto de las *Red Eléctrica Inteligente (REI)*. En particular, el grupo de reguladores europeos de electricidad y gas; Describe las *REI* o *SG* como *"Una red eléctrica que puede integrar el comportamiento y las acciones de todos los usuarios conectados de una forma eficiente en cuanto a costos, incluyendo productores, consumidores y actores que son tanto productores como consumidores, para asegurar una red eléctrica que haga un uso mas eficiente de los recursos a un costo inferior, asegurando menores perdidas y mayor calidad y seguridad de la demanda".* [11].

Por su parte, el *Instituto Nacional de Estándares y Tecnología de Estados Unidos (NIST)*; Concibe una *SG* como *"Una red moderna con flujo bidireccional de energía que provee, mediante comunicaciones bidireccionales y capacidades de control, una serie de funcionalidades y*

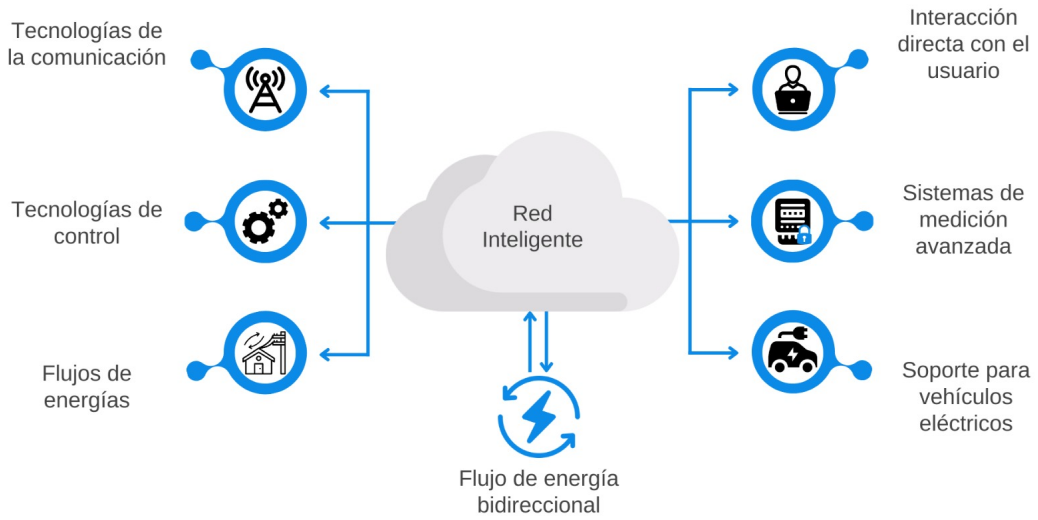
aplicaciones a la red"[12]. El *Electric Power Research Institute (EPRI)* adopta la definición; La *SG* es la *"Modernización del suministro eléctrico, para lo cual se debe monitorear, proteger y optimizar automáticamente la operación de los elementos interconectados a ella, desde la generación (tanto si esta es centralizada como distribuida), pasando por la red de transporte y distribución hasta los consumidores industriales, sistemas automáticos en edificios, consumidores finales y sus equipos (vehículo eléctrico, electrodomésticos, etc.)" [13].*

2.2.1 Aspectos clave de las REI

La integración de diversas tecnologías es fundamental para la implementación de una red inteligente o Smart Grid, con el fin de generar beneficios tanto para proveedores de energía como para operadores de *Tecnologías de la Información y la Comunicación (TIC)* y usuarios finales. Este sistema combina comunicación, control y electrónica avanzada para transformar la red eléctrica tradicional en una infraestructura digital interoperable, caracterizada por una mayor confiabilidad, flexibilidad, disponibilidad y reducción de costos energéticos.

En este contexto, las *REI* se configura como la modernización digital del sistema eléctrico, integrando *Tecnologías de la Información y la Comunicación*, *Tecnologías de la Operación (TO)* y recursos energéticos distribuidos en todas las etapas de generación, transmisión, distribución y consumo. Su arquitectura permite un flujo bidireccional de energía e información, habilitando esquemas de gestión de la demanda, aprovechamiento de recursos renovables locales y la participación activa de los usuarios como productores mediante la *Generación Distribuida.*

Figura 2.1: Smart Grid en el sector TIC.



Fuente: Elaboración propia.

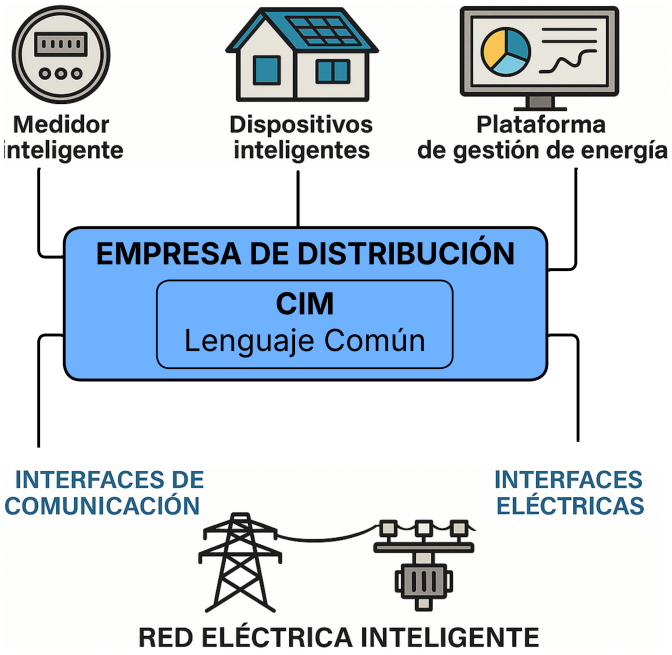
Entre los componentes clave destacan la *AMI*, que optimiza la gestión energética mediante medidores inteligentes y comunicación en tiempo real; el concepto *Vehicle-to-Grid (V2G)*, que ofrece almacenamiento distribuido y aporta flexibilidad en escenarios de alta demanda; y la *ciberseguridad*, elemento esencial para garantizar la integridad, disponibilidad y confidencialidad de los datos, así como la continuidad del suministro frente a ciberamenazas.

Instituciones como el *NIST* y experiencias internacionales, como la de Suecia, subrayan que la *SG* no constituye únicamente una mejora tecnológica, sino una infraestructura diseñada para afrontar los desafíos energéticos del siglo XXI. Mediante dispositivos como *Phasor Measurement Unit (PMU)*, *Remote Terminal Unit (RTU)*, *Industrial Internet of Things (IIoT)* y sistemas de automatización avanzada, se consolida una plataforma flexible que soporta aplicaciones como tarifas dinámicas, mercados energéticos digitalizados y soluciones de eficiencia operativa.

2.2.2 Modelo Conceptual e Interoperabilidad

Un modelo conceptual en las *Smart Grid (SG)* es una abstracción para comprender y analizar sistemas complejos, identificando sus elementos y relaciones. Su objetivo es ofrecer una visión estructurada para la planificación, el diseño y la integración de tecnologías en el sistema eléctrico.

Figura 2.2: Arquitectura basada en el modelo CIM.



Fuente: Elaboración propia

2.2.2.1 Modelo Conceptual del CIM

El *Common Information Model (CIM)* es una herramienta clave para establecer un lenguaje común que represente los datos del *Sistema Eléctrico de Potencia (SEP)*, facilitando la comunicación entre sistemas de *Tecnologías de la Información (IT)* y *Tecnologías de la Operación (OT)*. Este modelo asegura la interpretación consistente de información esencial, como el consumo, la producción y la gestión de red entre diferentes sistemas. El *CIM* es un conjunto de estándares internacionales de la *International Electrotechnical Commission (IEC)* que normaliza la representación de datos y el intercambio de información en el *SEP*. Estas normativas, las cuales se presentan en la Tabla 2.1, generalmente establecen un lenguaje común para la interoperabilidad entre sistemas de gestión de energía, distribución y el mercado energético, facilitando el intercambio de información entre organizaciones del sector [14].

El *CIM* es esencial para la interoperabilidad en las *SG*, al proporcionar un lenguaje común que normaliza la representación e intercambio de datos del *SEP* y facilita la integración entre sistemas *IT* y *OT*. Sin embargo, requiere complementarse con estándares de ciberseguridad, como la IEC 62351, que garantizan la confidencialidad, integridad y disponibilidad de la información en entornos de comunicación bidireccional. En este contexto, normativas, guías técnicas y marcos legales buscan alinear estrategias para una gestión energética interoperable y segura, asegurando la comunicación confiable entre dispositivos inteligentes y la integración eficiente de recursos.

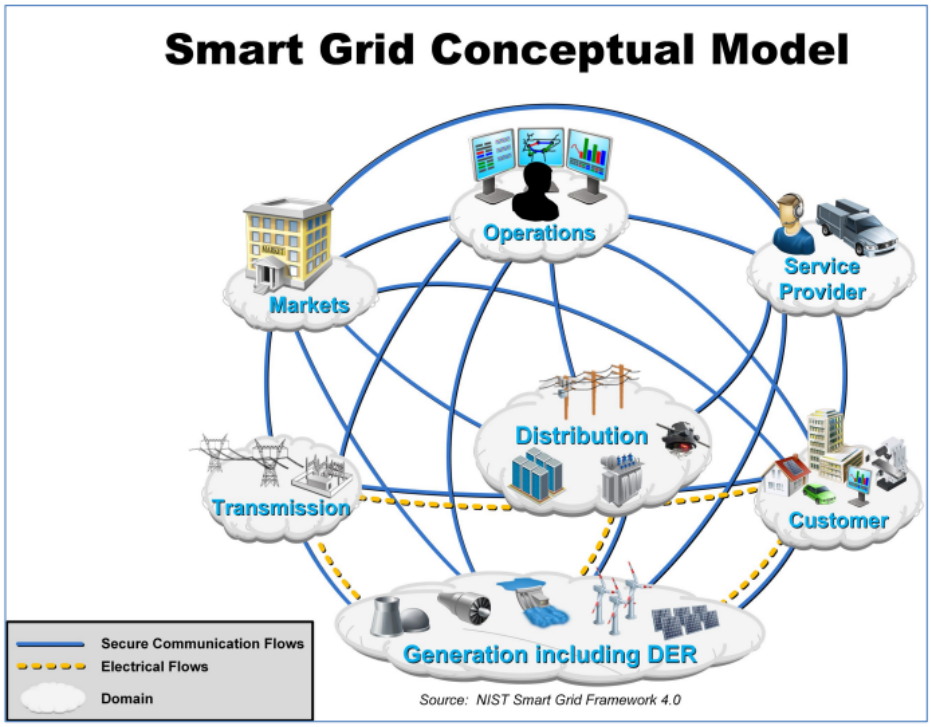
Tabla 2.1: Estándares IEC para Smart Grids [14, 15, 16, 17]

Estándar	**Descripción**	**Propósito/Ámbito**
IEC 61970	Modelo de datos para representar componentes del Sistema Eléctrico de Potencia *SEP*, centrado en el intercambio de información entre sistemas de operación y planificación de la red.	Facilita la interacción entre actores del sistema eléctrico, como generadores, transformadores y consumidores, asegurando un flujo de datos eficiente.
IEC 61968	Estándar que abarca el intercambio de información entre sistemas de distribución, apoyando funciones como monitoreo, control y atención al cliente del sistema eléctrico.	Permite la interoperabilidad entre sistemas diversos mediante la definición de interfaces, garantizando la integración en la operación y mantenimiento de la red.
IEC 62325	Estándar que regula el intercambio de información entre los participantes del mercado eléctrico, incluyendo datos meteorológicos, contratos y precios.	Enfocado en la operación del mercado eléctrico, gestionando aspectos como facturación, capacidad de transmisión y otros datos operacionales clave.

2.2.2.2 Modelo de Interoperabilidad del NIST

El modelo de interoperabilidad del *NIST* proporciona una representación de las interacciones en una *SG*, descrita en el documento Framework and Roadmap for Smart Grid Interoperability Standards [18], hoy referencia internacional para empresas eléctricas. Su enfoque permite identificar actores y relaciones dentro de los siete dominios de la *SG*: generación, transporte, distribución, consumo, mercado, operación y servicios, como se observa en la **Figura 2.3** [19].

Figura 2.3: Modelo Conceptual y dominios de la Smart Grid (SG).



Fuente: Tomado de [20]

2.2.2.3 Interacción Entre Dominios

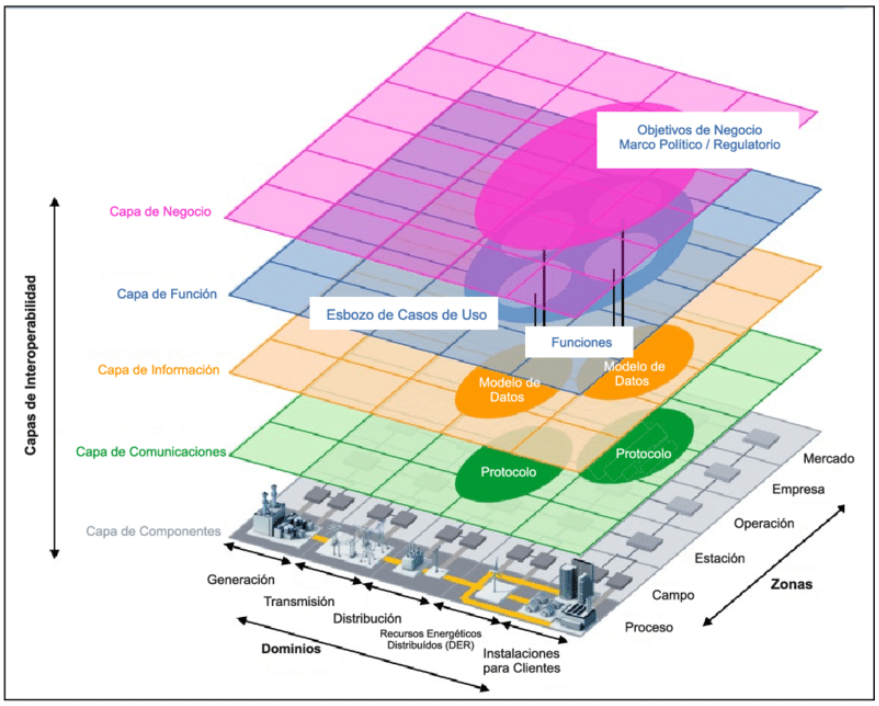
Los dominios del modelo de interoperabilidad en las redes eléctricas inteligentes (*REI*) se definen por su función y sus relaciones con otros dominios. Los actores de cada dominio operan tecnologías como medidores inteligentes y sistemas de control. A su vez, las interfaces eléctricas y de comunicación permiten la interconexión entre ellos, creando una red dinámica y flexible.

Tabla 2.2: Dominios del Modelo Conceptual de Smart Grids [21, 22]

Dominio	Descripción	Tecnologías/Actores
Generación	Este dominio incluye plantas tradicionales como recursos *DER* y fuentes renovables. Los actores en este dominio son responsables de la producción de electricidad y su distribución.	Plantas de generación convencional, DER, fuentes renovables, sistemas de almacenamiento de energía, inversores, medidores inteligentes.
Transporte	Se encarga de la infraestructura de transmisión de alta tensión y subestaciones que controlan el flujo de energía en la red.	Subestaciones de alta tensión, redes de comunicación para monitoreo en tiempo real.
Distribución	Este dominio se ocupa de la entrega final de energía a los consumidores. Gestiona subestaciones y las líneas de distribución.	Subestaciones, transformadores, líneas de distribución, medidores inteligentes.
Consumo	Representa al usuario final, que puede ser hogares, empresas o instalaciones industriales.	Medidores inteligentes, dispositivos de control de consumo, plataformas de gestión de la demanda.
Mercado	Este dominio gestiona las transacciones de energía, contratos de compra-venta y la integración de actores.	Comercializadores y plataformas de negociación de energía, sistemas de gestión de contratos.
Operación	Se refiere a la supervisión y el control en tiempo real de la red, asegurando que la energía fluya de manera eficiente y confiable.	Sistemas SCADA, *SGO*, sistemas de control de estabilidad de la red.
Servicios	Este dominio abarca servicios adicionales como la optimización del consumo energético y gestión de la demanda.	Integración de (V2G), servicios de gestión de la demanda, plataformas de optimización energética.

El *GridWise Architecture Council (GWAC)* desarrolló un modelo de referencia conceptual para facilitar la identificación de estándares y protocolos de interoperabilidad técnica y seguridad informática en los sistemas eléctricos modernos [22]. Este modelo estructura las capas desde la infraestructura física y software básico hasta los protocolos y aplicaciones y las funciones de negocio, formando una arquitectura escalonada [23].

Figura 2.4: Modelo arquitectural SGAM.



Fuente: Tomado de [24]

2.2.2.4 Interacción Entre Capas

El modelo conceptual del NIST destaca la relevancia de las interfaces eléctricas y de comunicación para la interconexión de los distintos dominios de la red. Las primeras permiten el flujo físico de energía entre generación, subestaciones y usuarios, mientras que las segundas habilitan el intercambio de datos y el control bidireccional mediante tecnologías como Ethernet, Wi-Fi, redes móviles o *PLC*.

En este marco, los protocolos de comunicación (ZigBee, Modbus, DNP3, *PLC*) son esenciales para la interoperabilidad entre medidores inteligentes, sistemas de control y plataformas de gestión. A su vez, los módulos Gateway cumplen la función de puentes entre sistemas heterogéneos, garantizando la comunicación, integridad y seguridad de los datos. El modelo de interoperabilidad es jerárquico. Cada capa depende de las capas inferiores para funcionar correctamente. Este modelo es escalable y modular, lo que significa que nuevos componentes o funcionalidades pueden añadirse a la red sin alterar las capas ya existentes.

Tabla 2.3: Capas del Modelo Conceptual de Smart Grid

Capa	Descripción	Tecnologías/Actores
1. Capa de Componentes	Equipos y dispositivos para la generación, almacenamiento y distribución de energía.	Generadores, paneles solares, baterías de almacenamiento, líneas de transmisión y subestaciones.
2. Capa de Comunicaciones	Intercambio de información entre dispositivos y sistemas, utilizando diferentes protocolos.	Modbus, DNP3, ZigBee, Power Line Communication (PLC), Wi-Fi, protocolos de comunicación IoT.
3. Capa de Función	Sistemas SCADA, plataformas de gestión de energía y sistemas de control de demanda.	SCADA, plataformas de gestión de energía, dispositivos de control de demanda inteligente.
4. Capa de Negocio	Herramientas de análisis de datos, predicción de demanda y servicios de usuarios finales.	Plataformas de análisis de datos, software de predicción, servicios de gestión de la demanda.

2.3 Ciberseguridad en Smart Grids y AMI

La convergencia entre *IT* y *OT* es esencial para la modernización de las redes eléctricas, pero incrementa la superficie de ataques, ya que la mayor conectividad del *IIoT* expone las redes a ciberamenazas. En este escenario, garantizar una interoperabilidad segura se ha vuelto prioritario.

El mercado del *IIoT* muestra un crecimiento acelerado valorado en 263.520 millones de dólares en 2021 y con una proyección de 1,69 billones para 2030 impulsado por la necesidad de monitoreo y análisis en tiempo real de activos críticos [25]. El sector eléctrico es uno de los principales adoptantes de estas tecnologías, aunque su integración plantea retos de ciberseguridad: las *IT* priorizan la confidencialidad, mientras que las *OT* se enfocan en el *safety* y la disponibilidad, por lo que las estrategias tradicionales no siempre resultan compatibles. Las *SG* incorporan múltiples tecnologías desde *Intelligent Electronic Device (IED)* y medidores inteligentes hasta sistemas empresariales de gestión de energía que generan un volumen creciente de datos, acentuado por la integración de *Distributed Energy Resources (DER)*, sensores y prosumidores. Para manejar este flujo, se requieren estándares de interoperabilidad que eviten problemas de compatibilidad. El *CIM*, desarrollado inicialmente por el *Electric Power Research Institute (EPRI)* y luego adoptado por la *IEC*, proporciona un modelo común que facilita el intercambio de información entre aplicaciones, organizaciones y mercados energéticos.

2.3.1 Ciberseguridad en el Contexto de la Evolución de las Redes Eléctricas

Para introducir nuevos conceptos en el sector eléctrico, como la ciberseguridad, es fundamental comprender la evolución de las redes eléctricas y su transformación en la *REI*. La electricidad, desde la invención de la bombilla, ha sido un motor clave en la transformación de la sociedad y el progreso industrial. A lo largo del siglo XX, la energía eléctrica continuó evolucionando, impulsada por la creación de centrales eléctricas y el desarrollo de energías renovables para satisfacer la creciente demanda y buscar fuentes más sostenibles. Esta evolución llevó a la modernización de las redes eléctricas.

La *REI* integran tecnologías digitales y sistemas de comunicación avanzados para gestionar

eficientemente el flujo de energía y datos, garantizando mayor fiabilidad y optimización de los recursos energéticos. En esta transición, las compañías eléctricas han combinado las *OT*, como los sistemas *SCADA* con las *IT*. La convergencia de *IT* y *OT*, inicialmente independientes, es una característica clave de esta evolución. Sin embargo, esta mayor automatización introduce nuevos retos, especialmente en la seguridad de los sistemas de comunicación, control y operación. La interconexión de la infraestructura física la hace susceptible a ciberataques, como el incidente en Ucrania en 2015, donde un correo phishing logró conceder acceso a los sistemas *SCADA* y causó interrupciones en el suministro eléctrico. A medida que las redes eléctricas evolucionan con el uso crecient e de datos y tecnología, se exponen a más ciberataques, lo que resalta la importancia de la seguridad cibernética.

2.3.1.1 Estándares de Ciberseguridad en el Sector Eléctrico

Los estándares de ciberseguridad en el sector eléctrico abarcan un amplio espectro de áreas, desde el diseño seguro de sistemas, la gestión integral de riesgos, hasta la protección de dispositivos específicos y protocolos de comunicación. Algunos de los estándares más relevantes proporcionan marcos de referencia para fabricantes, operadores, integradores y reguladores, asegurando que las medidas de seguridad se implementen de manera coherente y efectiva. A continuación, se presenta una **Tabla 2.4** con los estándares más destacados que regulan la ciberseguridad en el sector eléctrico, describiendo brevemente sus objetivos principales y aspectos clave que abordan.

Tabla 2.4: Resumen de los principales estándares de ciberseguridad aplicados al sector eléctrico

Estándar	**Objetivo**	**Información relevante**
IEC 62351	Seguridad por diseño e integración de medidas para proteger protocolos críticos como IEC 61850 y IEC 60870.	Protege sistemas SCADA y responde a ciberataques como el Industroyer de 2016. [26, 27]
NERC CIP	Protección de activos críticos en sistemas de control y operaciones eléctricas.	Reconocido internacionalmente como referencia para protección de infraestructuras críticas. [?]
ISO/IEC 27001	Garantiza confidencialidad, integridad y disponibilidad de la información en organizaciones.	Proporciona un marco para la implementación efectiva de controles de seguridad. [28]
ISO 27019	Complementa ISO/IEC 27002 enfocándose en sistemas de control industrial del sector energético.	Adaptación del proceso de gestión de riesgos al contexto energético, mejora la resiliencia. [28]
IEC 62443	Protección integral para infraestructuras industriales críticas mediante seguridad por capas.	Promueve segmentación de redes y mejores prácticas para fabricantes e integradores. [29]
NISTIR 7628	Seguridad para redes inteligentes con enfoque en hardware y software.	Comparable en alcance a ISO/IEC 27019, enfocado en infraestructuras críticas. [30]
IEEE 1686	Evaluación y mitigación de riesgos en entornos de tecnologías operativas (OT).	Mejora la protección y resiliencia en infraestructuras digitales industriales. [31]

2.3.1.2 Estándares de Ciberseguridad en el Sector Eléctrico Colombiano

En Colombia, la ciberseguridad en el sector eléctrico es una prioridad fundamental para proteger la infraestructura crítica del país. Las principales medidas y normativas incluyen:

- Acuerdo 1960 del *Consejo Nacional de Operación (CNO)*: Inicialmente, el *Consejo Nacional de Operación (CNO)* aprobó, mediante el Acuerdo 1502 de 2021, la actualización

de la Guía de Ciberseguridad para el sector eléctrico colombiano [32], con el propósito de reforzar la protección de los ciberactivos críticos del *Sistema Interconectado Nacional (SIN)* y de establecer lineamientos para los agentes del sistema generadores, transmisores y distribuidores sobre la gestión de inventarios de ciberactivos, la realización de análisis de riesgos y vulnerabilidades, y la ejecución de planes de recuperación ante incidentes [33]. Posteriormente, en respuesta al incremento de las amenazas cibernéticas y a la evolución tecnológica del sector, el *CNO* expidió el Acuerdo 1960 de abril de 2025, mediante el cual se aprueba una nueva actualización de la Guía de Ciberseguridad [34]. Esta versión incorpora un enfoque basado únicamente en el cumplimiento normativo, promoviendo la adaptación de los controles de ciberseguridad al perfil de riesgo de cada agente del sistema eléctrico.

- Política Nacional de Seguridad Digital: Establece lineamientos orientados a fortalecer la gestión de riesgos digitales en ciudadanos, entidades gubernamentales y empresas, promoviendo una cultura de responsabilidad compartida frente a las amenazas cibernéticas. Asimismo, esta política reconoce la importancia de proteger infraestructuras críticas del país, incluyendo sectores estratégicos como el energético, con el fin de garantizar la continuidad de los servicios esenciales y aumentar la resiliencia frente a ciberataques.[35].

- Decreto 338 de 2022: Promulgado el 8 de marzo de 2022, establece los lineamientos generales para fortalecer la gobernanza de la seguridad digital en Colombia [32]. Su objetivo es mejorar la coordinación y respuesta ante incidentes, y promover la confianza y gestión del conocimiento en esta materia, creando el Modelo y las instancias de Gobernanza de Seguridad Digital para articular mejor a entidades públicas y privadas [36].

- CONPES 3701: Este documento actualiza también la Guía de Ciberseguridad para el sector eléctrico, con el fin de reforzar la protección de activos críticos frente a ciberamenazas [31]. Indica que los agentes del sistema (generadores y distribuidores) deben implementar medidas para identificar, proteger y gestionar los riesgos de sus ciberactivos [37].

2.3.1.3 Digitalización de la Energía: Un Nuevo Paradigma de Ciberseguridad

La transmisión de información crítica en las *Smart Grids* genera riesgos de alteración o robo de datos, lo que compromete la privacidad de los usuarios y puede tener graves consecuencias sociales y nacionales ante una interrupción del servicio eléctrico. De acuerdo con el NISTIR 7628, la digitalización de la red incorpora millones de componentes que deben garantizar la *Confidentiality, Integrity y Availability (CIA)* de la información, especialmente en comunicaciones bidireccionales. Los cibercriminales buscan vulnerar estos objetivos mediante técnicas de ataque que afectan la seguridad y estabilidad de la red. En este sentido, el propósito central de la ciberseguridad en las *SG* es asegurar el cumplimiento de los principios de *CIA* y, con ello, proteger la información y

la operación del sistema eléctrico. Para un enfoque integral, es necesario atender los objetivos y requerimientos ilustrados en la **Figura 2.5**.

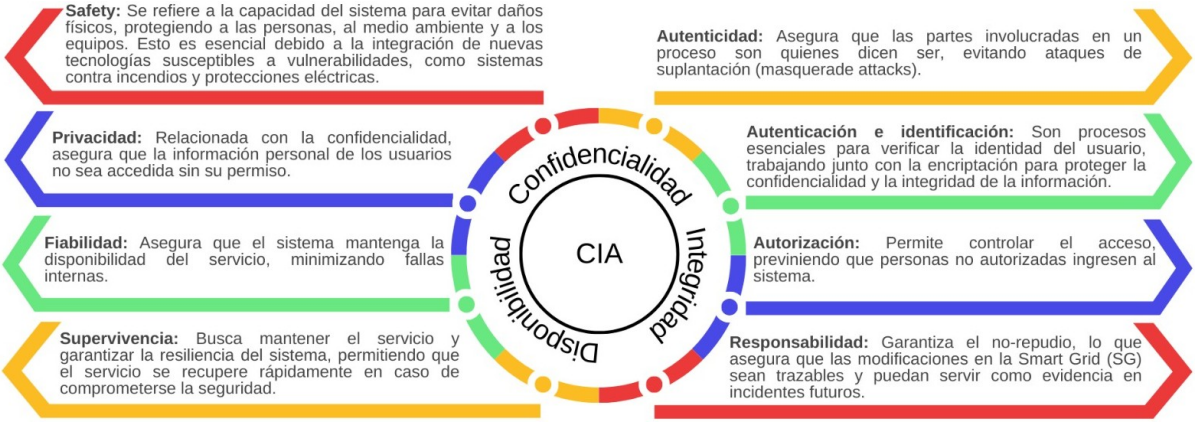
Figura 2.5: Objetivos y requerimientos de la ciberseguridad en Smart Grid.



Fuente: Tomado de [10]

Entre los requerimientos que aseguran la *CIA* en términos de ciberseguridad se destacan los siguientes que se describen a continuación en la **Figura 2.6**.

Figura 2.6: Requerimiento de la CIA en terminos de ciberseguridad.



Fuente: Elaboración propia.

Los ciberataques tienen como objetivo comprometer sistemas o acceder a información sensible mediante la explotación de vulnerabilidades en dispositivos o sistemas. Para ello, los cibercriminales suelen seguir un proceso estructurado que describe la progresión del ataque desde la identificación del objetivo hasta el mantenimiento del acceso. Este enfoque, ilustrado en la **Figura 2.7** presenta una secuencia general de cuatro etapas: reconocimiento, escaneo, explotación y mantenimiento del acceso. Esto permite comprender el comportamiento de los atacantes, así como identificar puntos clave para la detección y contención de amenazas antes de que afecten la operación de los sistemas.

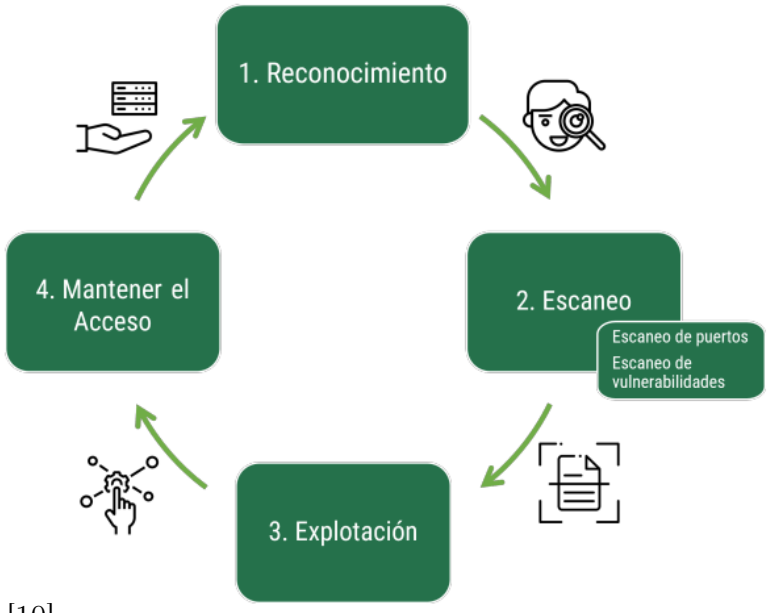
- **Reconocimiento:** En esta etapa inicial, los atacantes recopilan información relevante del objetivo mediante técnicas como la ingeniería social y el análisis de tráfico. La ingeniería social busca obtener credenciales o información confidencial a través de métodos como phishing o smishing, mientras que el análisis de tráfico permite identificar dispositivos y sistemas conectados a la red, por ejemplo, mediante técnicas de *eavesdropping*.

- **Escaneo:** Consiste en identificar los sistemas activos y los servicios disponibles en la red. Incluye el escaneo de direcciones IP, puertos, servicios y vulnerabilidades. Inicialmente, se detectan los dispositivos conectados, luego los puertos abiertos y posteriormente los servicios asociados, como los sistemas de control utilizados en subestaciones. A partir de esta información, los atacantes identifican vulnerabilidades que puedan ser explotadas.

- **Explotación:** En esta fase, los cibercriminales aprovechan las vulnerabilidades detectadas para obtener control del sistema. En el contexto de las Smart Grid (SG), se enfocan en componentes críticos como las unidades de control y plataformas de comunicación, empleando herramientas maliciosas como malware, ataques de Denegación de servicios (DoS), Man-In-The-Middle o Amenaza Persistente Avanzada (APT). Uno de los ataques más comunes es el Denegación de Servicio Distribuida (DDoS), cuyo objetivo es interrumpir la sincronización temporal de la red, fundamental para la detección de fallas y la localización de eventos.

- **Mantener el acceso:** Finalmente, los atacantes buscan garantizar un acceso persistente al sistema comprometido mediante la instalación de *backdoors* con privilegios elevados y el uso de *rootkits*, los cuales permiten ejecutar procesos de forma oculta y dificultan su detección por los mecanismos de seguridad tradicionales.

Figura 2.7: Secuencia de un ciberataque.



Fuente: Tomado de [10]

2.3.2 Revisión Bibliométrica Sobre Ciberseguridad en la Unidad de Medida

La primera etapa de la revisión bibliométrica se orientó a identificar literatura científica específicamente relacionada con ciberataques a sistemas de Medición Avanzada (AMI), con énfasis particular en la *Unidad de Medida (UM)* como elemento individual de la infraestructura. Para ello, se construyó una ecuación de búsqueda restringida que combinó términos asociados a *Advanced Metering Infrastructure*, *Smart Meter*, *Cybersecurity*, *Metering unit* y *Cyber attack*, aplicada en bases de datos de alto impacto como Scopus y Web of Science.

Tabla 2.5: Resultados de la ecuación de búsqueda específica de ciberseguridad en sistemas AMI.

#	Palabra clave	Ecuación	BBDD	Artículos	Repetidos
1	Advanced Metering Infrastructure	`(TITLE-ABS-KEY(Advanced Metering Infrastructure) AND TITLE-ABS-KEY(Smart Meter) AND TITLE-ABS-KEY(Cybersecurity) AND TITLE-ABS-KEY(Metering unit) AND TITLE-ABS-KEY(Cyber attack))`	Scopus	2	1
2	Smart Meter				
3	Cybersecurity				
4	Metering unit	Results for *Advanced Metering Infrastructure (Topic)* AND *Smart Meter (Topic)* AND *Cybersecurity (Topic)* AND *Metering unit (Topic)* AND *Cyber attack (Topic)*	WOS	4	1
5	Cyber attack				

Los resultados obtenidos evidencian una limitada disponibilidad de literatura en este dominio específico. En total, se identificaron únicamente seis documentos relevantes, de los cuales algunos correspondían a registros duplicados entre las bases de datos. Adicionalmente, el análisis del trabajo permitió constatar que la mayoría aborda la ciberseguridad en sistemas AMI desde una perspectiva sistémica, considerando la infraestructura completa, las redes de comunicación o los sistemas de gestión centralizada, sin profundizar en la unidad de medida como dispositivo individual.

Esta observación resulta especialmente relevante para el presente trabajo de grado, dado que el alcance experimental se centra exclusivamente en la unidad de medida operando en un entorno de laboratorio, con acceso a puertos locales y sin interacción con otros componentes de la infraestructura AMI, tales como concentradores de datos, redes PLC o sistemas de cabecera Head End System (HES). En este contexto, muchos de los mecanismos de seguridad descritos a nivel de infraestructura completa no son directamente transferibles al escenario de estudio, debido a que la superficie de ataque y las capacidades del dispositivo difieren. Por tanto, esta primera revisión bibliométrica no solo evidencia la escasez de trabajos enfocados en la ciberseguridad de la unidad de medida de forma individual. Esta ampliación permite identificar técnicas de ataque aunque no fueron concebidos originalmente para sistemas AMI, pueden ser adaptados y reinterpretados bajo las restricciones operativas propias de los medidores inteligentes y del protocolo DLMS/COSEM.

2.3.2.1 Revisión Bibliométrica General sobre Ciberseguridad y Ciberataques

La segunda etapa de la revisión bibliométrica se orientó a ampliar el alcance del análisis hacia el dominio general de la ciberseguridad, con el propósito de identificar, a partir de la literatura científica existente, los tipos de ataques que resultan más relevantes y en este campo, y que pueden ser adaptados al contexto de los sistemas de medición inteligente y a la unidad de medida.

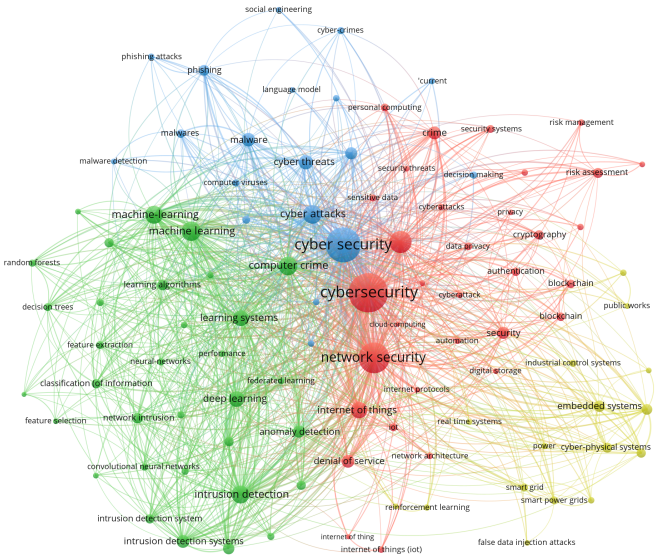


Figura 2.8: Bibliometría orientada a ciberseguridad

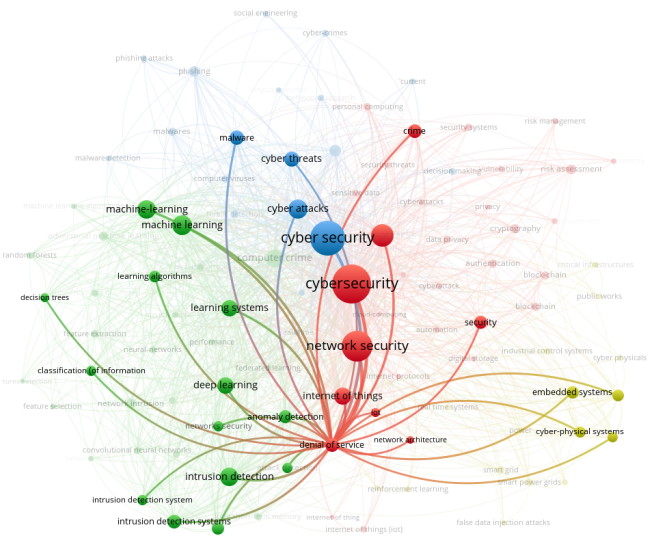


Figura 2.9: Bibliometría orientada a ciberseguridad (DoS)

Para esta etapa se construyó una ecuación de búsqueda de carácter amplio, empleando términos generales como *cybersecurity* y *cyber attack*, aplicada en bases de datos de alto impacto como Scopus y Web of Science. Los resultados obtenidos, resumidos en la Tabla 2.6, evidencian un volumen considerable de literatura científica de documentos asociados a estas temáticas, lo cual contrasta de manera significativa con la limitada literatura identificada en la revisión específica de sistemas AMI. El análisis de concurrencia de palabras clave, representado en la Figura 2.8, permite visualizar la estructura temática del campo de la ciberseguridad y las múltiples ramas de investigación que lo componen. En dicho mapa se identifican clústeres asociados a seguridad de redes, detección de intrusiones, aprendizaje automático, sistemas embebidos, Internet de las Cosas (Internet de las Cosas (IoT)) y sistemas ciberfísicos, entre otros. Estas áreas reflejan la diversidad de enfoques desde los cuales se estudian los ciberataques. Se observa de manera consistente la aparición del ataque Denegación de servicios (DoS) como uno de los vectores de ataque recurrentes en la literatura de ciberseguridad. Tal como se aprecia en la Figura 2.9, el DoS se posiciona como un nodo relevante que se conecta con áreas como seguridad de redes, sistemas distribuidos, IoT y sistemas ciberfísicos, lo que evidencia su importancia transversal en distintos dominios tecnológicos.

La identificación del ataque DoS en esta etapa de la revisión no implica que dicho ataque haya sido ampliamente estudiado en el contexto específico de sistemas AMI o de unidades de

medida inteligentes, sino que confirma su relevancia general dentro del campo de la ciberseguridad. Este resultado sustenta metodológicamente la selección del DoS como un tipo de ataque pertinente para ser analizado y adaptado al entorno de los medidores inteligentes, considerando las particularidades operativas, comunicacionales y de acceso que caracterizan a estos dispositivos. Esta segunda revisión bibliométrica cumple la función de establecer un puente entre la literatura general de ciberseguridad y su posible aplicación al ámbito de los sistemas de medición inteligente, proporcionando una base conceptual sólida para la selección del tipo de ataque abordado experimentalmente en este trabajo de grado.

Tabla 2.6: Resultados de la ecuación de búsqueda general en ciberseguridad y ciberataques.

#	**Palabra clave**	**Ecuación – Enfoque específico**	**BBDD**	**Artículos**
1	Cybersecurity	`(TITLE-ABS-KEY(cybersecurity) AND TITLE-ABS-KEY(cyber attack))`	Scopus	22380
2	Cyber attack	Results for *cyber attack (Topic)* AND *cybersecurity (All Fields)*	WOS	3386

2.3.2.2 Identificación Bibliométrica de Técnicas Asociadas a Ataques DoS

La tercera etapa de la revisión bibliométrica se orientó a la identificación de técnicas específicas para la ejecución de ataques de DoS, partiendo de que el DoS constituye el objetivo principal del ataque analizado en este trabajo de grado. En este contexto, las técnicas de *flooding* y *fuzzing* no fueron consideradas como categorías primarias dentro de la bibliometría, dado que la literatura suele priorizar el concepto general de DoS por encima de los mecanismos técnicos que lo materializan. No obstante, a partir del análisis detallado de la literatura, se identificó que tanto el *flooding* como el *fuzzing* son técnicas ampliamente utilizadas para provocar condiciones de agotamiento de recursos, degradación del servicio y pérdida de disponibilidad en sistemas informáticos y de comunicación. Estas técnicas se entienden como mecanismos derivados del DoS, cuyo propósito es explotar debilidades en la gestión de tráfico, validación de entradas o manejo de recursos del sistema objetivo. Un soporte relevante para esta selección se encuentra en el trabajo *"Malware Exploitation and Vulnerability Assessment of CVE-2024-38063 in Windows 10 and 11 in Academic Networks Cybersecurity" [38]*, donde los autores emplean de manera explícita técnicas de *fuzzing* a nivel de aplicación y *flooding* mediante fragmentación IPv6 para generar estrés operativo y condiciones de denegación de servicio. Los resultados reportados evidencian picos críticos de uso de CPU, degradación del rendimiento y deficiencias en la validación de entradas, aun en sistemas actualizados y parcheados, demostrando que estas técnicas son efectivas para inducir escenarios DoS sin requerir una explotación directa de vulnerabilidades críticas. A partir de esta evidencia, se justifica la adopción de técnicas de *fuzzing* y *flooding* como mecanismos experimentales para la ejecución del ataque DoS en la unidad de medida del sistema AMI. Aunque estas técnicas no emergen de forma explícita como palabras clave dominantes en la bibliometría general, su relevancia se sustenta en la literatura especializada como herramientas

prácticas para evaluar la resiliencia y disponibilidad, permitiendo trasladar estos enfoques al contexto de los medidores inteligentes y su infraestructura de medición avanzada.

2.4 Laboratorios de Sistemas AMI

Los laboratorios dedicados a las *SG* y a la *AMI* son componentes estratégicos de innovación tecnológica, ya que permiten probar, simular, validar y certificar nuevas tecnologías antes de su implementación a gran escala. Estos laboratorios integran múltiples disciplinas, como electrónica de potencia, telecomunicaciones, ciberseguridad, automatización, análisis de datos y gestión energética, lo que los convierte en espacios para la innovación y el desarrollo tecnológico del sector eléctrico. La evolución de las redes eléctricas hacia sistemas más inteligentes y resilientes requiere infraestructuras de soporte que garanticen la interoperabilidad, el cumplimiento de estándares y el correcto funcionamiento de los dispositivos, siendo los laboratorios *AMI* fundamentales para la validación de medidores inteligentes, concentradores de datos, *HES*, protocolos de comunicación y esquemas de respuesta a la demanda. Estos laboratorios fortalecen las capacidades humanas e institucionales al promover la formación y la transferencia de conocimiento entre los sectores académico, industrial y gubernamental.

2.4.1 Revisión de Laboratorios de Smart Grid y AMI

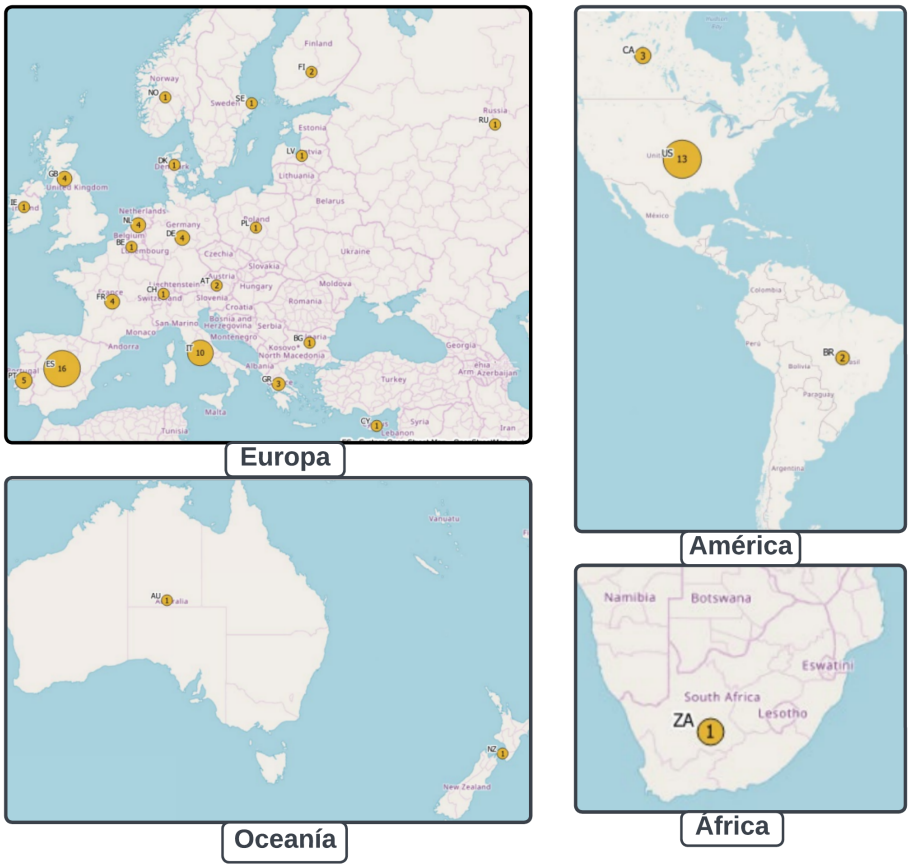
El informe del *Joint Research Centre (JRC)* [39] sobre el inventario de laboratorios de redes inteligentes en 2022 muestra un panorama global, pero con una notable predominancia de laboratorios europeos (65 de 86), lo que indica el papel destacado de Europa en la transición energética. La Unión Europea ha promovido activamente políticas y la inversión en tecnologías de redes inteligentes, lo que ha impulsado la creación de numerosos laboratorios en esta área. Si bien los laboratorios europeos comparten un enfoque en áreas prioritarias para la UE (interoperabilidad, ciberseguridad, integración de renovables), también exhiben una diversidad de enfoques, influenciada por los sistemas energéticos y las políticas de cada país. El informe *JRC* destaca la colaboración entre países de la UE en investigación e innovación energética, a través de redes y proyectos conjuntos. Estos laboratorios suelen contar con infraestructuras de vanguardia y financiamiento significativo, lo que les permite desarrollar soluciones innovadoras.

El informe destaca la importancia de la participación de laboratorios de Norteamérica y otras regiones en la investigación global de redes inteligentes por varias razones. La diversificación de perspectivas y enfoques es clave: Norteamérica aporta su experiencia con diversos sistemas eléctricos, y la inclusión de regiones como África, Asia, Australia y Latinoamérica (Brasil) amplía el espectro de conocimientos. Cada región enfrenta desafíos y prioridades únicas, lo que enriquece la investigación, promueve el intercambio de ideas y permite adaptar soluciones a diferentes contextos. Esta participación asegura que las soluciones sean más robustas y globalmente relevantes. Además, la inclusión de regiones en desarrollo resalta prioridades como la

asequibilidad y la creación de capacidades locales. Un análisis de la literatura revela que la información sobre una gran cantidad de laboratorios de redes inteligentes se encuentra principalmente en el inventario del *JRC*. Este inventario reúne datos de 86 laboratorios a nivel mundial, proporcionando información precisa sobre sus respectivas áreas de trabajo. Un enfoque significativo de estos laboratorios (47 %) se centra en la medición avanzada *AMI*. El informe estructura la información de los laboratorios en cinco grupos de tecnologías definidos por la plataforma *European Technology and Innovation Platforms Smart Networks for Energy Transition (ETIP SNET)* y adoptados por la Comisión Europea, e incluye: Integrated Grid que abarca *AMI*, Customers and Market, Storage, Generation, y Digitalización, Comunicación y Datos. Las categorías y subcategorías establecidas por *ETIP SNET*.

Se examinó una muestra de 86 laboratorios de *SG*, con una concentración significativa con 65 en Europa. A pesar de esta predominancia europea, el informe indica que el estudio incluyó la comunicación con laboratorios de varias regiones a nivel global. En la **Figura 2.10** se puede observar la ubicación geográfica de los laboratorios por continente y la cantidad de cada uno de ellos por región. En la **Figura 2.10** se puede observar la ubicación geográfica de los laboratorios por continente y la cantidad de cada uno de ellos por región.

Figura 2.10: Laboratorios por el continente de Europa, América, Oceanía y África.

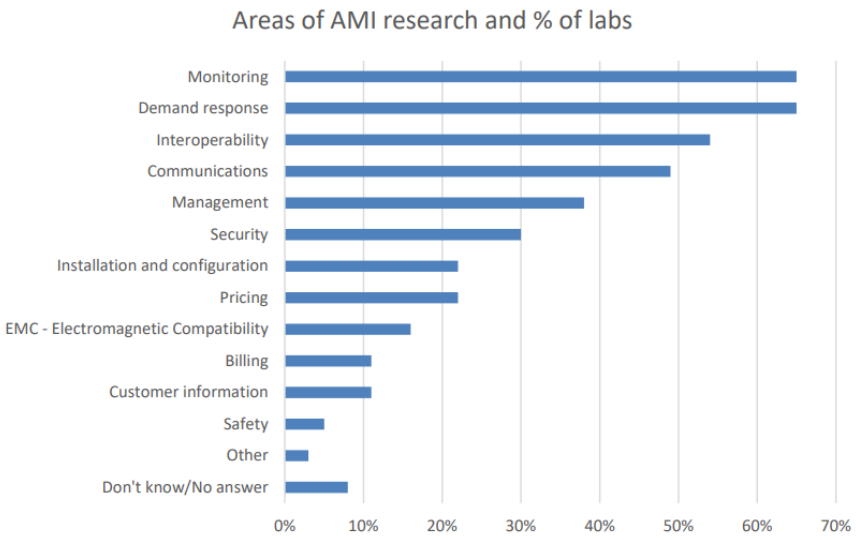


Fuente: Tomado de [39]

En la siguiente **Figura 2.11** se muestra las áreas de investigación y los porcentajes de

laboratorios con los temas relacionados con *AMI*. Los temas con mayor atención en los laboratorios que investigan son: el monitoreo y la respuesta a la demanda, presentes en el 65 % de los casos. Les siguen la interoperabilidad 54 % y las comunicaciones 49 %, lo que evidencia el interés en funciones para la gestión moderna de redes eléctricas.

Figura 2.11: Áreas de investigación de AMI y porcentaje de laboratorios.



Fuente: Tomado de [39]

2.4.2 Normas Técnicas Bajo las Cuales Están Acreditados los Laboratorios

Los datos obtenidos, revelan una diversidad de situaciones en cuanto a la acreditación de los laboratorios. Si bien un 20 % de los laboratorios afirmó contar con las acreditaciones correspondientes y un 69 % indicó no tenerlas, es importante destacar que un 11 % optó por no responder a la pregunta. Esta falta de respuesta, sumada al alto porcentaje de laboratorios sin acreditación, sugiere la necesidad de una mayor investigación sobre las razones detrás de esta situación, Las normas acreditadas por laboratorios son presentados en la **Tabla 2.7**. No obstante, para aquellos laboratorios que sí proporcionaron información sobre su acreditación, se mencionan varias de las normas bajo las cuales están certificados. Se presenta un desglose detallado de las normativas citadas por los laboratorios, así como el número de laboratorios que cuentan con cada una de ellas. Este análisis es fundamental para entender qué tan alineados están los laboratorios con los estándares internacionales, y cómo esto influye en su capacidad para realizar investigaciones y validaciones tecnológicas dentro del campo de las redes inteligentes.

Tabla 2.7: Normas acreditadas por laboratorios [39]

Norma	Nº de laboratorios
IEC 17025	5
IEC 61850	2
ISO 9001	2
UNE-EN 62052	1
UNE-EN 62053	1
UNE-EN 61000	1
IEC 60870-5	1
IEC 61131-3	1

El área de *AMI* forma parte del grupo de trabajo de red integrada, lo que resalta su importancia dentro de los estudios sobre la modernización de las redes eléctricas. Dado que requieren un enfoque multidisciplinario y el cumplimiento de normas internacionales para garantizar su interoperabilidad y funcionamiento eficiente, resulta fundamental destacar las normativas que guían el trabajo de los laboratorios en esta área. La **Tabla 2.8** proporciona un resumen de las normas que los laboratorios emplean para abordar los temas relacionados con la red integrada, especificando el porcentaje de laboratorios que las aplican en sus investigaciones. Estas normas cubren aspectos técnicos y de comunicación para el desarrollo de sistemas que permitan la integración de distintas tecnologías.

Tabla 2.8: Estándares aplicados para los laboratorios [39]

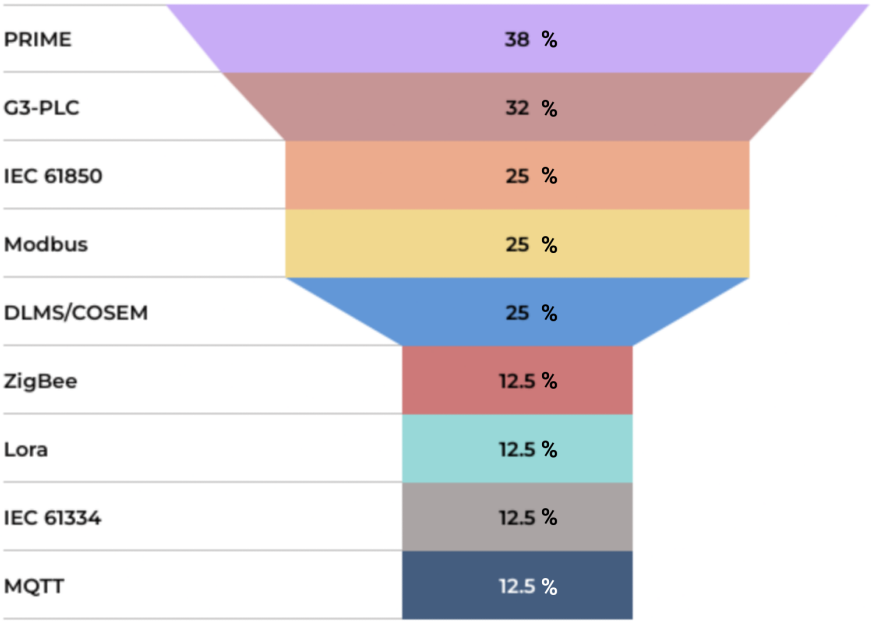
Norma	% de laboratorios
IEC 61850 - Communication networks and systems in substations	77 %
IEC 61970 - Common Information Model / Energy Management	23 %
IEC 61968 - Common Information Model / Distribution Management	20 %
IEC 60870 - Telecontrol equipment and systems	11 %
IEC 1547 - IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces	11 %
CEI 0-16 (national codes)	9 %
CEI 0-21 (national codes)	9 %
IEC 61869 - Instrument transformers	9 %
IEC 60255-24 - Electrical relays – COMTRADE	6 %
IEC 62325 - Common Information Model (CIM) for Energy Markets	6 %
IEEE 1588 - Precision Time Protocol	6 %
IEC 60947 - Low-voltage switchgear and controlgear	6 %
Open ADR – Open Automated Demand Response	6 %

En el contexto de *AMI*, se abordan diversos temas de estudio, tecnologías y normativas aplicadas. En la investigación sobre el documento se pueden observar las tecnologías de comunicación de datos utilizadas en los laboratorios que investigan *AMI*, junto con los porcentajes de laboratorios que implementan cada una de ellas. Entre estas tecnologías, las comunicaciones inalámbricas destacan como la opción más utilizada, con un 57 % de los laboratorios activos en *AMI* empleándolas en sus investigaciones. Sin embargo se encuentran las soluciones de comunicación cableada, como fibra óptica, cobre y *Power Line Communications (PLC)*, utilizadas por el 54 % y 37 % de los laboratorios. Estos porcentajes reflejan la adopción de

diferentes enfoques para garantizar la eficiencia de la comunicación en los sistemas, cada uno con sus ventajas y desafíos, dependiendo del tipo de red y la infraestructura disponible.

La **Figura 2.12** detalla las normas y tecnologías que emplean los laboratorios dedicados a *AMI*, así como el porcentaje de participación de cada una de ellas en sus investigaciones. Es crucial hacer una distinción entre las tecnologías y los medios de comunicación utilizados en estos sistemas. Mientras que los medios de comunicación se refieren a los canales físicos a través de los cuales se transmite la información, como fibra óptica, *PLC* o comunicaciones inalámbricas, las tecnologías se refieren al modelado de los datos y las plataformas de software que gestionan, analizan y procesan esta información.

Figura 2.12: Normas y tecnologías aplicadas para laboratorios AMI.



Fuente: Adaptado de [39]

En la **Tabla 2.9** se presentan las normas y tecnologías utilizadas por al menos un laboratorio en el ámbito de *AMI*. Esta tabla incluye una lista de las principales normativas y tecnologías implementadas, como IEC 60255, NB-IOT, OSGP, LoraWan, Ethernet, WiFi, entre otras. Estas tecnologías abarcan tanto protocolos de comunicación, como estándares de medición, reflejando la diversidad de enfoques utilizados por los laboratorios para abordar la infraestructura de medición avanzada. Cada norma y tecnología mencionada es empleada por al menos un laboratorio en sus investigaciones y pruebas dentro del área *AMI*.

Tabla 2.9: Normas utilizadas por al menos un laboratorio [39]

Norma	Tecnologías	Actores
IEC 60255	NB-IOT	OSGP
IEC 62056	LoraWan	Interbus
IEC 870-5-102, -103	Ethernet	RS485
EN 50470-1, -3	Cellular	OPC DA
EN 62053-21, -22, -23, -24	DNP3	M2M
IEEE 1901	WiFi	DCSK
IEEE 1588-PTP	Bluetooth	Bacnet
IEEE C37.112	RF-Mesh	MQTT

2.4.2.1 Respuesta de la Demanda

La respuesta de la demanda es un área prioritaria de investigación, con el 86 % de los laboratorios activos en este campo según el *JRC*. Se refiere a programas que incentivan a los usuarios a modificar su consumo de energía en función de precios o incentivos, incluyendo subcategorías como flexibilidad distribuida, gestión de carga y dispositivos finales. Entre las tecnologías más usadas destaca *Open Automated Demand Response (OpenADR)*. En el contexto colombiano, la respuesta de la demanda resulta clave para enfrentar la variabilidad climática, el aumento en el consumo y la integración de energías renovables. Su aplicación permite reducir la congestión de la red, optimizar la operación del sistema y disminuir costos, además de empoderar a los consumidores como actores activos del mercado eléctrico. Finalmente, es esencial determinar qué modelos de respuesta (basados en precios, incentivos directos o control directo) se ajustan mejor a las particularidades del sistema y los usuarios nacionales.

Tabla 2.10: Normas y laboratorios en AMI [39]

Laboratorio	Protocolos/Norma	Referencia
DNV	DLMS	[40]
TECNALIA	PRIME	[41]
KEMA-CESI	IEC 60255-11/31, IEC 62053-11/21/22/23/24, IEC 62055-31, IEC 60255-31, PLC	[42]
TRIALOG	G3-PLC	[43]
ITE	PRIME	[44]
SILICON LABS	Wireless	[45]
SMS	Wired and wireless radio technologies	[46]
SINFET	Smart Home Management System	[47]
CCLAB	Security requirements, IEC 62443	[48]
APPLUS LABORATORIES	Security requirements, Accredited IT Security Evaluation Facility (ITSEF)	[49]
CEPRI	Validación	[50]
EDP Labelec	PLC/PRIME, PLC/BPL	[51]
UFD	Interoperabilidad	[52]
Kalkitech	Interoperabilidad	[53]
TÜV Rheiland	Interoperabilidad, wireless, Technology ANSI C12	[54]

2.5 Laboratorios de Ciberseguridad: Análisis de DoS en AMI

El estudio de ataques de *DoS* y su variante distribuida *Denegación de Servicio Distribuida (DDoS)* en la *Advanced Metering Infraestructure (AMI)* requiere entornos de prueba controlados que combinen técnicas de simulación, emulación y experimentación con hardware físico. Estos laboratorios permiten evaluar el impacto real de los ciberataques en la red eléctrica y validar la eficacia de los mecanismos y estrategias de defensa antes de su implementación en campo [55].

2.5.1 Equipos y Hardware Utilizados

1. Plataformas de prueba (*Testbeds*) ciberfisicas: Son entornos experimentales que integran simultáneamente componentes cibernéticos (protocolos, tráfico de red, simulación de ataques) y físicos (hardware de medición, routers, sensores). Estas plataformas permiten analizar cómo un ataque afecta tanto la comunicación como la operación eléctrica, aportando una visión integral de la seguridad del sistema [56]. Además, constituyen un recurso clave para validar la resiliencia de la red *AMI* bajo escenarios realistas [55].
2. Emulación de medidores inteligentes mediante SBCs: Se emplean computadoras de placa única (SBCs), como Raspberry Pi o BeagleBone [55], configuradas con radios IEEE 802.15.4 y sistemas ligeros basados en Linux. Estos dispositivos permiten emular las capacidades computacionales y de comunicación de un medidor inteligente real, incluyendo limitaciones de procesamiento, memoria y energía. Su uso facilita la recreación de ataques de DoS a gran escala sin necesidad de exponer equipos comerciales en producción [55].
3. Infraestructura de red: Los laboratorios reproducen la topología completa de una red *AMI*, incluyendo enrutadores, switches, cortafuegos, servidores y *Unidad de Concentracón de Datos (DCU)*. Esta infraestructura permite analizar la propagación de los ataques y observar cómo afectan a los diferentes niveles de comunicación: *Red de Área Domestica (HAN)*, *Red de Área de Vecindario (NAN)* y *Red de Área Amplia (WAN)* [57].
4. Herramientas de ataque: Para simular escenarios de *Denegación de servicios (DoS)/Denegación de Servicio Distribuida (DDoS)*, se utilizan programas de código abierto, ampliamente empleados en ciberseguridad; Uno de los programas es *Hping3 y Scapy* , el cual es para generar trafico TCP/UDP/ICMP malicioso [58]; el siguiente es *CommView Visual Packet Builder* , el cual es para construir paquetes de red personalizados [59]; y *BoNeSi (Botnet Network Simulator)* , que permite recrear ataques *DDoS* a gran escala controlando miles de bots virtuales [60, 61].

2.5.2 Software de Simulación y Emulación para el Análisis de DoS/DDoS

En el ámbito de la ciberseguridad para la *AMI*, el uso de herramientas de simulación y emulación resulta fundamental para analizar los efectos de ataques de *Denegación de Servicio (DoS/DDoS)* y validar mecanismos de defensa. Estos entornos permiten reproducir escenarios

realistas a gran escala, evaluar la resiliencia de los protocolos de comunicación y probar algoritmos en condiciones controladas. La **Tabla 2.11** resume los principales simuladores empleados en la literatura, destacando su alcance para el estudio de amenazas en redes *AMI*.

Tabla 2.11: Software de simulación y emulación para el análisis de DoS/DDoS en AMI

Herramienta	Descripción y aplicaciones
Network Simulator 3 (NS-3)	Simulador de eventos discretos de código abierto ampliamente utilizado para modelar entornos de red AMI a gran escala. Permite simular redes con cientos o miles de nodos y puede emplearse en co-simulación con hardware físico mediante modelos como *TapBridge*.
OMNeT++ y MiXiM	Frameworks de simululación empleados en la implementación y evaluación de ataques DoS en redes inalámbricas. MiXiM ofrece módulos especializados para modelar comunicaciones en escenarios AMI.
NeSSi2	Entorno de simulación basado en agentes, orientado al análisis de seguridad en redes. Permite evaluar mecanismos como Sistemas de Detección de Intrusiones (IDS) y simular escenarios de ataque específicos, incluyendo tormentas UDP y otros tipos de inundación de tráfico.
OPNET	Herramienta de simulación ampliamente utilizada en el análisis de redes AMI. Se emplea para modelar la comunicación de medidores inteligentes y estudiar el impacto de ataques DDoS sobre distintos protocolos de enrutamiento, evaluando métricas como retardo, congestión y disponibilidad del sistema.

2.5.3 Normativas de Protocolos Relevantes en AMI

Aunque la literatura técnica no siempre hace referencia explícita a "normativas" en el sentido de marcos regulatorios gubernamentales, sí describe los estándares de comunicación y protocolos que constituyen la base operativa de la Infraestructura de Medición Avanzada (AMI). Estos estándares son, al mismo tiempo, los objetivos principales de ataques *Denegación de servicios (DoS)/Denegación de Servicio Distribuida (DDoS)* y el foco de estudio en plataformas de prueba y laboratorios de ciberseguridad.

- Protocolos de comunicación inalámbrica

    1. IEEE 802.15.4 / IEEE 802.15.4g: Son estándares fundamentales para redes de área de vecindario (NAN) *Red de Área de Vecindario (NAN)* y *Red de Área Domestica (HAN)*. Definen el nivel físico y de enlace de datos, y son ampliamente empleados en tecnologías como *ZigBee y Wi-SUN*. En entornos experimentales de ciberseguridad, estos protocolos se utilizan para emular la comunicación de bajo consumo entre medidores inteligentes y concentradores de datos, reflejando con fidelidad sus limitaciones en ancho de banda, potencia de transmisión y capacidad de procesamiento [55].
    2. ZigBee: Uno de los protocolos pioneros en las primeras implementaciones de *AMI*. A pesar de haber surgido como una solución orientada al bajo consumo y al bajo costo, continúa teniendo relevancia en el ámbito de las redes *HAN* debido a su compatibilidad con IEEE 802.15.4 y su uso extendido en sistemas *IoT* [55]..
    3. WiMAX *(World interoperability for microwave access)*: Representa una opción robusta para las *Red de Área Amplia (WAN)* que conectan múltiples *NAN* con los servidores centrales de las compañías eléctricas. Con un alcance de hasta 50 km y tasas de

transmisión que pueden llegar a 70 Mbps, proporciona un canal adecuado para la transmisión masiva de datos de medición [62].

4. Tecnologías celulares (4G/5G): Cada vez más utilizadas en despliegues modernos de *AMI*, estas tecnologías permiten la conexión de medidores y unidades concentradoras a través de infraestructuras de telecomunicaciones ya existentes. El uso de redes celulares ofrece ventajas en cobertura y escalabilidad, pero introduce riesgos adicionales asociados a la exposición al Internet público [62].

2.5.4 Protocolos de Enrutamiento

Los ataques de *Denegación de servicios (DoS)* dirigidos a infraestructuras *AMI* suelen aprovechar debilidades inherentes a los protocolos de enrutamiento ad hoc, que son esenciales para la comunicación en redes malladas de medidores inteligentes. Entre ellos destacan:

- Dynamic Source Routing (DSR): Este protocolo es uno de los principales objetivos del denominado *Puppet Attack*, donde un atacante manipula un nodo legítimo para que inunde la red con mensajes de descubrimiento de rutas (RREQ) de alta prioridad. El resultado es la saturación del ancho de banda y el agotamiento energético de los dispositivos, sin que el atacante genere directamente el tráfico malicioso [63].

- Ad hoc On-Demand Distance Vector (AODV) y Destionation Sequenced Distance Vector (DSDV): Estos protocolos también han sido ampliamente analizados en escenarios de laboratorio, ya que presentan vulnerabilidades frente a ataques de inundación y manipulación de tablas de enrutamiento. En particular, en entornos *AMI*, la manipulación de mensajes de enrutamiento puede provocar la pérdida de conectividad, latencias excesivas y caídas parciales de la red, comprometiendo la transmisión de datos críticos, como medidas de consumo o comandos de control [64].

2.5.5 Ataque de Denegación de Servicio DoS

La disponibilidad es un pilar fundamental de la ciberseguridad en las *Smart Grids*, buscando garantizar que los usuarios tengan acceso confiable a los recursos y la información en todo momento [64]. La pérdida de esta disponibilidad puede resultar directamente en la interrupción del servicio y del acceso a datos críticos en una *SG*, lo que podría tener consecuencias graves para el correcto funcionamiento del sistema eléctrico. En la actualidad, la dependencia de la información en tiempo real para el monitoreo, la toma de decisiones y la gestión eficiente del Sistema Eléctrico de Potencia (*SEP*) hace que cualquier interrupción sea crítica.

Uno de los ataques más frecuentes y dañinos contra la disponibilidad de los sistemas es la Denegación de Servicio (DoS), cuyo objetivo es saturar los enlaces de comunicación y afectar

recursos críticos como servidores y bases de datos. Estas técnicas buscan interrumpir, deteriorar o ralentizar el flujo de información [65, 66]. Un caso emblemático fue el malware Industroyer, que explotó la vulnerabilidad CVE-2015-5374 en los relés de protección SIPROTEC de Siemens, impidiendo la recepción de comandos hasta que se realizara un reinicio manual, lo que dejaba al dispositivo fuera de operación. Este tipo de ataque está clasificado por MITRE ATT&CK bajo la técnica Denial of Service (DoS, ID: T0814) [67]. Muchos protocolos de comunicación en las *SG* se basan en IP (Internet Protocol), como el IEC 61850 que utiliza TCP/IP, lo que los hace vulnerables a ataques de Denegación de Servicio (DoS) y Denegación de Servicio Distribuido (DDoS), afectando directamente la disponibilidad. La amplia adopción de protocolos como IEC 61850 para la digitalización de subestaciones, la comunicación de recursos distribuidos y microrredes amplifica esta vulnerabilidad. En el caso específico de los medidores inteligentes de *Advanced Metering Infraestructure (AMI)*, los Jamming Attacks son una preocupación. El objetivo principal de estos ataques es inhabilitar la comunicación de los medidores con la empresa proveedora del servicio, lográndolo mediante la interferencia de los medios inalámbricos de comunicación con señales de ruido [68]. Esto puede afectar a los medidores de dos maneras: el canal de comunicación puede ser ocupado constantemente por los routers, o los paquetes de datos pueden ser bloqueados e impedidos de ser recibidos [69]. Adicionalmente, los cibercriminales pueden aprovechar tecnologías vulneradas en la *SG* para crear una red de dispositivos comprometidos, la cual usarían para lanzar ataques DDoS dirigidos a otras organizaciones, afectando su infraestructura cibernética.

2.5.5.1 La Amenaza de Ataques de DoS en AMI

Los ataques *Denegación de servicios (DoS)* y su variante *Denegación de Servicio Distribuida (DDoS)* constituye una de las amenazas critica para *AMI* [55]. Este ataque tiene como finalidad afectar la disponibilidad de los datos y servicios, bloqueando el acceso de los usuario legítimos a los recursos de la red y generando interrupciones en la operación del sistema eléctrico [55].

La vulnerabilidad se ve incrementada por la fuerte dependencia del sistema *AMI* respecto a las redes de comunicación inalámbricas, las cuales, a pesar de su flexibilidad y bajo costo de despliegue, son altamente susceptibles a congestión deliberada de canales, interferencias y saturación por tráfico malicioso [55, 70]. En este sentido, los medidores inteligentes representan objetivos especialmente expuestos, dado que operan con recursos computacionales limitados y se comunican mediante protocolos y bandas frecuentemente utilizados en entornos abiertos, lo que facilita el monitoreo y potencial manipulación de sus tramas de datos. La evidencia respalda la magnitud de este riesgo; diversos estudios señalan que hasta un 80 % de las empresas eléctricas han experimentado al menos un ataque de tipo *DoS* en sus infraestructuras [71, 62], en muchos casos con un alcance masivo y consecuencias que van desde la perdida temporal de comunicación hasta la afectación de procesos

críticos de supervisión y control. Estos incidentes no solo comprometen la continuidad del servicio, sino que también pueden deteriorar la confianza de los usuarios y generar perdidas económicas significativas para las compañías distribuidoras.

2.5.5.2 Mecanismos de Ataque DoS/DDoS en Sistemas AMI

En las redes *AMI*, los ataques de *Denegación de servicios (DoS)* y su variante *Denegación de Servicio Distribuida (DDoS)* pueden ejecutarse mediante diferentes técnicas que buscan saturar los recursos de comunicación y computo, afectando la disponibilidad de los servicios. A continuación, se describen los métodos mas comunes:

1. Ataques de inundación (*Flooding Attacks*)
    - Inundación del canal inalámbrico: Es uno de los procedimiento mas frecuentes. El atacante emplea un transmisor para generar un volumen masivo de señales de interferencia o paquetes de red ficticios *dummy packets*, cuyo propósito es congestionar los canales de comunicación de los medidores inteligentes [55]. Como consecuencia, se interrumpe la comunicación bidireccional con los enrutadores de la red (*grid routers*), lo que impide tanto el envío de comandos desde el centro de control como la transmisión del estado operativo de los medidores [55]. Este tipo de ataque se aprovecha de la naturaleza compartida y abierta de los medidores inalámbricos, donde es difícil diferencia trafico legitimo de trafico malicioso.
    - Inundación de protocolos *(SYN, UDP, ICMP)*: Estos ataques explotan vulnerabilidades inherentes a protocolos. Por ejemplo, en un ataque de inundación SYN el adversario envía miles de solicitudes de conexión TCP que el servidor intenta procesar sin éxito, saturando sus recursos hasta volverlo inaccesible para usuarios legítimos [62]. De manera similar, las inundaciones basadas en UDP o ICMP generan un trafico masivo de paquetes de sobrecarga el ancho de banda disponible y degrada el rendimiento de la red.
    - Ataque de repetición (*Replay Attack*) de alta tasa: En este caso, el atacante captura paquetes validos de comunicación y los reenvía repetidamente a gran velocidad. Aunque los paquetes son auténticos en cuanto a su estructura y contenido, el exceso de trafico puede desbordar las capacidades de procesamiento de nodos intermedios y servidores, generando una denegación de servicio [62]. Este mecanismo resulta especialmente peligroso porque el trafico malicioso se camufla como legitimo, dificultando su detección.
    - Ataque RTS (*Request to Send*): Propio de redes *Red de Área Local Inalámbrica (WLAN)*, consiste en que un nodo malicioso transmite tramas de control RTS al punto de acceso, solicitando acceso exclusivo al canal de comunicación por un tiempo prolongado. Al reservar de manera fraudulenta el medio, lo que ocasiona una generación de servicio

generalizada [72].

2. Ataques de marioneta (*Puppet Attack*): El denominado ataque de marioneta representa una modalidad de *Denegación de servicios (DoS)* particularmente sigilosa y eficiente dentro de las redes de *Advanced Metering Infraestructure (AMI)* [73]. En este escenario, el atacante no genera directamente el trafico malicioso de inundación; en su lugar, selecciona un nodo legitimo de la red y lo convierte en una *"marioneta"*. Para ello, envía paquetes diseñados de forma especifica que engañan al nodo comprometido [62], el cual comienza a retransmitir masivamente paquetes de enrutamiento de alta prioridad, como las solicitudes de descendimiento de rutas *(RREQ)* del protocolo DRS.

   El efecto inmediato es la congestión de los canales de comunicación, el agotamiento del ancho de banda y el consumo acelerado de la energía de los dispositivos implicados [62, 63]. Este tipo de ataque resulta difícil de detectar, ya que el trafico malicioso proviene de un nodo aparentemente normal, lo que complica la identificación del verdadero origen de la amenaza [73]. De hecho, investigaciones muestran que la tasa de entrega de paquetes en un escenario bajo ataque de marioneta puede descender drásticamente hasta niveles del 20 % o incluso 10 %, comprometiendo gravemente la disponibilidad del servicio.

3. Ataques basados en agentes (Botnets): Los ataques *Denegación de Servicio Distribuida (DDoS)* en entornos *AMI* suelen materializarse mediante el uso de *botnets*, un mecanismo organizado en dos fases principales.
   - Reclutamiento de agentes: El atacante infecta una gran cantidad de medidores inteligentes con *malware*, transformándolos en nodos *zombie* o *bots* [74, 75]. Estos dispositivos, al igual que otros elementos del internet de las cosas *IoT*, suelen estar expuestos debido a limitaciones en sus capacidades de seguridad y a configuraciones de protección insuficientes [76].
   - Fase de ataques: Una vez conformada la *botnet*, el atacante coordina de manera remota a todos los medidores comprometidos para ejecutar un ataque de inundación de forma simultanea. El objetivo habitual son componentes críticos como las *DCU* o los servidores centrales de la empresa eléctrica [74]. El atacante resulta devastador, ya que aprovecha la capacidad de miles de dispositivos distribuidos para generar un flujo masivo de trafico malicioso que puede colapsar los sistemas de gestión y supervisión de la red.

2.5.5.3 Consecuencia de un Ataque DoS/DDoS en Sistemas AMI

Las repercusiones de un ataque sobre una red *AMI* son de gran severidad y pueden extenderse más allá de la simple interrupción de comunicaciones:

- Pérdida de comunicación: El centro de control queda imposibilitado de enviar comandos esenciales, como ordenes de desconexión remota o actualizaciones de tarifas dinámicas [55].

- Pérdida de datos de medición: La utilidad eléctrica deja de recibir información sobre el consumo en tiempo real, lo que impacta negativamente en la facturación, el pronostico de carga y la planificación operativa [75].
- Inestabilidad de la red: La ausencia de datos confiables y de capacidad de control en tiempo real puede incluir a errores en la toma de decisiones, afectando la estabilidad del sistema eléctrico [58]. En escenarios extremos, este tipo de ataques podría incluso desembocar en apagones generalizados [62].

2.6 Síntesis

Este capítulo logró consolidar los conceptos fundamentales relacionados con AMI, ciberseguridad y ataques de denegación de servicio, proporcionando el soporte teórico necesario para el desarrollo del estudio. Se abordaron los componentes de la infraestructura AMI, el rol de la unidad de medida, los protocolos de comunicación involucrados y los principios de ciberseguridad aplicables a infraestructuras críticas. De esta manera, el capítulo permitió establecer un marco de referencia que facilita la comprensión de los riesgos, amenazas y vulnerabilidades presentes en los sistemas de medición avanzada.

3. METODOLOGÍA PARA UNA PRUEBA DE VULNERABILIDAD

3.1 Introducción

Este capítulo define los requisitos necesarios para la realización de una prueba de vulnerabilidad de *Denegación de servicios (DoS)* aplicada a medidores inteligentes. Desde una perspectiva de ciberseguridad, los medidores inteligentes constituyen activos críticos debido a su rol como puntos de acceso entre el dominio físico del sistema eléctrico y las redes de comunicación utilizadas para supervisión, facturación y control.

El desarrollo del capítulo se estructura en torno a la identificación de las superficies de ataque relevantes en la comunicación del medidor, considerando tanto los aspectos físicos de transmisión como los protocolos lógicos que gestionan el intercambio de información. Para este propósito, se utiliza el modelo OSI como marco de referencia. Este enfoque es fundamental para delimitar el alcance de las técnicas de ciberseguridad que pueden aplicarse de manera realista en un entorno *AMI*. A partir de este análisis, el capítulo presenta la propuesta de la prueba, en la cual se seleccionan técnicas de ciberseguridad orientadas a la denegación de servicio. Las técnicas consideradas como flooding, fuzzing se adaptan al protocolo DLMS/COSEM y al modelo de operación secuencial de los medidores inteligentes. Dichas técnicas no se plantean como ataques genéricos, sino como estímulos controlados que permiten estudiar la reacción del dispositivo frente a cargas elevadas de solicitudes válidas o tramas alteradas. Finalmente, se definen los requisitos técnicos para la ejecución de la prueba. Se describen las características relevantes del software de comunicación DLMS del medidor inteligente utilizado, de la carga fantasma empleada para simular condiciones eléctricas reales y del equipo computacional que actúa como generador de tráfico. La definición de estos elementos es para garantizar que la prueba se realice en un entorno controlado. La metodología para la ejecución de la prueba de vulnerabilidad se estructura a partir de un diagrama general que integra las etapas conceptuales y técnicas del estudio. Dicho diagrama se presenta de forma consolidada en el **Anexo 5.1** y en el Anexo **Anexo 5.2** por secciones que sirve como guía para la organización desarrolladas en este capítulo.

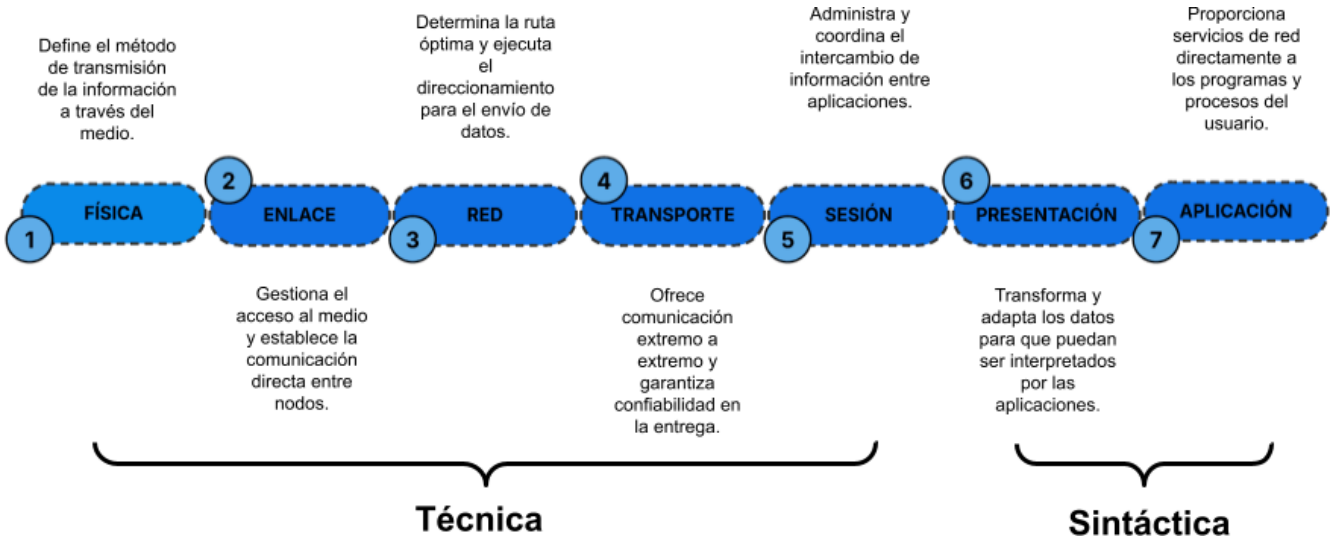
3.1.1 Infraestructura de Medición Avanzada (AMI) en el contexto del modelo OSI

El modelo *Open Systems Interconnection (OSI)* constituye una referencia fundamental para comprender cómo se estructura, organiza y transmite la información dentro de cualquier sistema de comunicaciones. Aunque los medidores inteligentes y las *Advanced Metering Infraestructure (AMI)* emplean protocolos especializados como *Device Language Message Specification/Companion Specification for Energy Metering (DLMS/COSEM)*, su funcionamiento

puede interpretarse de manera clara si se analiza bajo el marco conceptual del modelo *OSI*, dado que este modelo descompone la comunicación en siete capas. En el contexto de *AMI*, las capas inferiores del modelo *física, enlace y red* adquieren relevancia porque determinan cómo se transmite la información desde el medidor hacia el concentrador. Tecnologías como PLC, RF, G3-PLC o puertos ópticos corresponden a estas capas y definen las propiedades eléctricas, la modulación, el acceso al medio y el direccionamiento. Estas capas permiten que los paquetes lleguen desde un dispositivo de campo hasta la infraestructura de la red *AMI* con fiabilidad.

Las capas superiores *transporte, sesión, presentación y aplicación* son para entender cómo se organiza la comunicación lógica entre el cliente y el medidor. *DLMS/COSEM*, que es el protocolo adoptado internacionalmente para la comunicación con medidores inteligentes, se ubica principalmente en estas capas, ya que define cómo se establece una sesión, cómo se intercambian objetos COSEM, cómo se asegura la integridad de las tramas y de qué manera se interpretan y gestionan los datos. En particular, la capa de aplicación es crítica porque es donde residen las estructuras *Sistema de Identificación de Objetos (OBIS)*, los perfiles de carga, los eventos y los servicios de lectura y escritura que permiten interactuar con el medidor. La separación entre las capas técnicas (1–4) y las capas sintácticas (5–7), resaltada en la **Figura 3.1**, permite comprender que en *AMI* no solo importa el medio físico por el cual se transporta la información, sino también la forma en que los datos son estructurados y procesados por el dispositivo. Esta organización es clave cuando se analizan escenarios de ciberseguridad, ya que cada capa puede presentar vulnerabilidades propias.

Figura 3.1: Modelo OSI



Fuente: Tomado de [8]

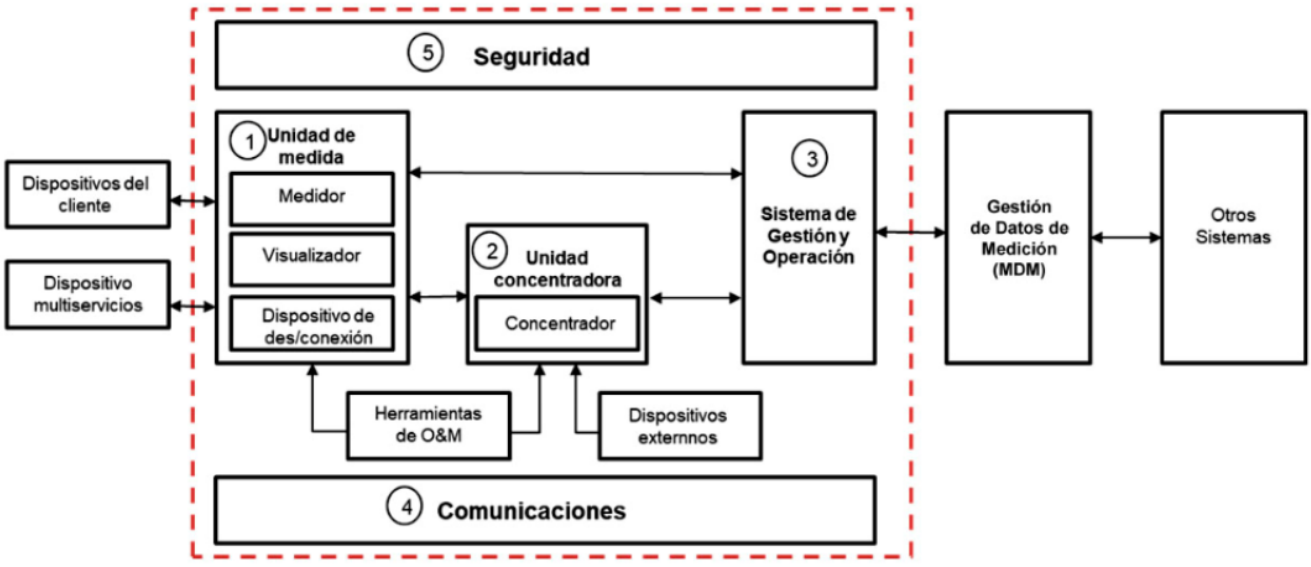
3.2 AMI (Advance Metering Infraestructure)

Las *Advanced Metering Infraestructure (AMI)* constituyen un pilar fundamental dentro de las *Smart Grids*, ya que conforman el sistema encargado de la medición y gestión inteligente de la energía. Su función principal es habilitar la comunicación bidireccional entre los medidores inteligentes instalados en los puntos de consumo y los sistemas centrales de la empresa eléctrica.

Gracias a esta interacción, es posible enviar, recibir y procesar en tiempo real los datos de consumo de los usuarios, lo que no solo optimiza la facturación y la previsión de la demanda, sino que también facilita operaciones avanzadas sobre la red, como la gestión de la demanda, la detección de fallas, la integración de *Distributed Energy Resources (DER)* y la implementación de tarifas dinámicas. En este sentido, los sistemas *Advanced Metering Infraestructure (AMI)* no son únicamente una infraestructura de medición, sino un mecanismo estratégico para la modernización del sistema eléctrico, mejorando su eficiencia, confiabilidad y capacidad de respuesta frente a los retos de la transición energética.

Según las arquitecturas más comunes para este tipo de sistemas, incluyen los siguientes componentes:

Figura 3.2: Arquitectura del sistema AMI.



Fuente: Tomado de [8]

3.2.1 Unidad de Medida (UM)

La *Unidad de Medida (UM)* constituye uno de los componentes más relevantes y exigentes del sistema *AMI*, debido a su papel como origen de toda la información del proceso de medición. Este

dispositivo recopila, registra y transmite los datos eléctricos hacia las redes de comunicación que posteriormente son enviados al *Sistema de Gestión y Operación (SGO)* para su procesamiento y análisis. La medición bidireccional es una característica esencial de la *UM*, ya que permite registrar tanto la energía consumida como la entregada, lo cual es indispensable para la operación de redes inteligentes y la integración de fuentes las *DER*. De acuerdo con la *NTC 6079*, la *UM* está compuesta por el medidor de energía eléctrica, los dispositivos de conexión y desconexión, el visualizador, y los medios que permiten al usuario acceder a la información de su consumo. Adicionalmente, pueden integrarse elementos complementarios como los dispositivos del cliente final o equipos multiservicios, aunque estos no se contemplan dentro del alcance normativo para el caso Colombiano, siendo únicamente con fines informativos [8].

3.2.2 Sistema de Gestión y Operación (SGO) o Head End System (HES)

El *Sistema de Gestión y Operación (SGO)*, también conocido como *Head End System (HES)*, es el núcleo del sistema *AMI*, encargado de la administración, supervisión y control de su operación. Integra aplicaciones de software para la recolección, almacenamiento y gestión de la información proveniente de las *Unidad de Medida (UM)*, incluyendo datos de consumo, eventos y comandos de conexión y desconexión. Asimismo, garantiza la continuidad operativa, el tratamiento de alarmas y la gestión de las comunicaciones, permitiendo el monitoreo y la trazabilidad en tiempo real. El *SGO* se integra con plataformas complementarias como la de *Gestión de datos de medición (MDM)*, los sistemas comerciales y las herramientas de mantenimiento de la red de distribución.

3.2.3 Unidad Concentradora (UC)

La *Unidad Concentradora (UC)* es un componente del sistema *AMI* que actúa como elemento intermedio entre las *Unidad de Medida (UM)* y el *SGO*. Su función principal es administrar la red de comunicación con los medidores, consolidar la información de medición y facilitar el intercambio de datos y comandos de control. Dependiendo de la tecnología y arquitectura del sistema, la *Unidad Concentradora (UC)* puede operar como un *gateway*, estar conformada por uno o varios concentradores, o incluso no ser necesaria cuando existe comunicación directa con el *SGO*. En todos los casos, desempeña un papel clave en la interoperabilidad y el flujo seguro de datos.

3.2.4 Comunicaciones

El sistema de comunicaciones es un componente transversal del *AMI* que garantiza el intercambio confiable, seguro y bidireccional de información entre las *UM*, las *UC* y el *SGO*. Según la infraestructura adoptada, la comunicación puede realizarse de forma directa o a través de las *UC*. De acuerdo con la norma *NTC 6079*, los medios de comunicación se clasifican en cableados e inalámbricos. Los primeros incluyen tecnologías como puertos eléctricos, *PLC* y fibra óptica, mientras que las comunicaciones inalámbricas abarcan interfaces ópticas para acceso local

y tecnologías de radiofrecuencia, las cuales permiten enlaces flexibles y de amplio alcance mediante topologías punto a punto, estrella o malla.

3.2.5 Seguridad

La seguridad en los sistemas *AMI* es una funcionalidad transversal que debe integrarse en todos sus componentes para garantizar una operación confiable y la protección de la información. Su implementación se fundamenta en la seguridad por diseño, la defensa en profundidad y la gestión de riesgos, enfoques que permiten proteger la confidencialidad, integridad y disponibilidad de los datos frente a amenazas y vulnerabilidades.

3.3 Medidor inteligente (Smart Meter)

Un *Smart Meter* es un dispositivo electrónico avanzado utilizado para registrar, almacenar y transmitir información precisa y continua sobre el consumo de energía eléctrica. Aunque el término puede extenderse a la medición de otros recursos como el gas o el agua, su aplicación más extendida se encuentra en el ámbito de la energía eléctrica.

El medidor inteligente constituye un elemento fundamental dentro de la *Advanced Metering Infraestructure (AMI)*, la cual forma parte integral del concepto de la *Red Eléctrica Inteligente (REI)*. Sin embargo, por sí solo no constituye una red inteligente, ya que requiere la integración con otros componentes, tales como sensores, actuadores, sistemas de comunicación y domótica, para garantizar la operación coordinada, eficiente y segura del sistema eléctrico [77, 78]. A diferencia de los medidores electromecánicos convencionales, los medidores inteligentes disponen de capacidad de comunicación bidireccional, permitiendo el intercambio de información entre el usuario final y la empresa distribuidora del servicio. Esta comunicación puede establecerse mediante diferentes tecnologías tales como, PLC, que utiliza la red eléctrica existente para la transmisión de datos *Wi-SUN y Wi-Fi*, basadas en enlaces inalámbricos de corto alcance; Redes móviles (LTE, NB-IoT, 5G), utilizadas para la comunicación en entornos urbanos o de gran escala [79].

Dicha infraestructura permite al medidor inteligente enviar datos de consumo, parámetros eléctricos, eventos y alarmas hacia un sistema central, donde la información es procesada, analizada y utilizada para optimizar la gestión operativa, detectar pérdidas, realizar mantenimiento predictivo y mejorar la confiabilidad del suministro. Adicionalmente, los medidores inteligentes cuentan con funcionalidades avanzadas de control remoto, tales como la conexión o desconexión del servicio eléctrico, la configuración dinámica de tarifas, y la detección de irregularidades o manipulación del medidor [80].

En el contexto normativo colombiano, la *Comisión de Regulación de Energía y Gas (CREG)* y

el ICONTEC, mediante la Norma Técnica Colombiana *NTC 6079:2021*, establecen las definiciones y especificaciones aplicables a los Sistemas *AMI*. En esta norma, el medidor inteligente de energía se define como un dispositivo capaz de registrar de forma detallada el consumo energético, realizar la conexión o desconexión remota del servicio, y utilizar una infraestructura de comunicaciones bidireccional para transmitir la información registrada hacia la empresa de servicios o el cliente, pudiendo además recolectar y almacenar datos de otros medidores o dispositivos [81, 8].

En el desarrollo de este trabajo de grado, el acceso al medidor inteligente se realiza exclusivamente a través de puertos locales, dado que la prueba se ejecuta en un entorno de laboratorio y se cuenta únicamente con la unidad de medida, sin conexión a una infraestructura AMI desplegada. En particular, se utiliza el puerto serial RS-485 como interfaz principal de comunicación. Desde el punto de vista físico, el puerto local utilizado en esta prueba se encuentra expuesto y accesible sin requerir mecanismos adicionales. A diferencia de otros elementos del medidor que pueden estar protegidos mediante tapas selladas, interruptores internos o alarmas de apertura, el puerto local no genera eventos de seguridad ni alarmas al establecer una conexión directa. Esto convierte al puerto en uno de los pocos puntos de acceso que interactúa con el medidor sin activar mecanismos de detección.

Desde el contexto de la ciberseguridad, esta exposición física incrementa la relevancia del puerto local como superficie de ataque. A través del puerto RS-232 es posible establecer sesiones DLMS completas y acceder directamente al protocolo de aplicación del medidor, sin la intermediación de capas adicionales de red. Mediante esta interfaz se pueden realizar operaciones de lectura y escritura sobre objetos identificados por códigos *OBIS*, consultar perfiles de carga, acceder a registros de eventos y obtener parámetros instantáneos del sistema eléctrico.

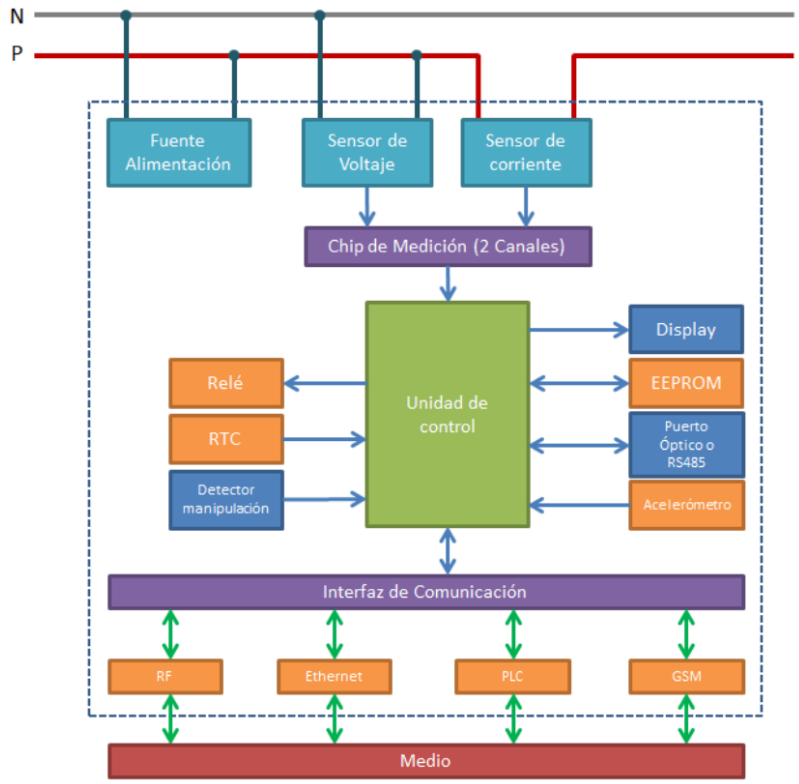
3.3.1 Componentes principales del medidor inteligente

Desde un punto de vista funcional, un medidor inteligente está compuesto por distintos módulos que interactúan de manera integrada para cumplir funciones de medición, control, comunicación y seguridad:

- Fuente de alimentación: transforma y estabiliza la energía proveniente de la red eléctrica para suministrar tensión regulada. Incorpora mecanismos de protección contra sobretensiones y fluctuaciones, garantizando la operación continua del dispositivo [82].
- Sensores de corriente y voltaje: capturan las magnitudes eléctricas fundamentales (corriente, tensión y potencia), que son digitalizadas por el chip de medición. Estos sensores permiten registrar tanto el flujo de energía activa como reactiva, asegurando precisión conforme a los estándares metrológicos [83].

- Chip de medición: componente encargado de realizar la conversión analógica–digital y el cálculo de parámetros eléctricos como potencia, energía acumulada y factor de potencia [82].
- Unidad de control (microcontrolador): es el núcleo lógico del medidor. Coordina la adquisición de datos, la ejecución de comandos, la comunicación con sistemas externos y la detección de eventos. Implementa rutinas de sincronización temporal mediante el reloj de tiempo real (RTC) y gestiona las funciones de seguridad.
- Módulos auxiliares:
    - RTC (Real Time Clock): mantiene la referencia temporal para el registro de históricos, alarmas y eventos.
    - Relé de corte: posibilita la desconexión y reconexión remota del suministro eléctrico, característica usada en esquemas de control de carga y sistemas de prepago.
    - Detector de manipulación: detecta intentos de apertura, golpes o inversión de polaridad mediante acelerómetros o sensores magnéticos.
    - Memoria EEPROM: almacena configuraciones, históricos de consumo y eventos de medición sin pérdida ante cortes de energía.
    - Display: proporciona al usuario información de consumo, alarmas o parámetros operativos en tiempo real.
- Interfaz de comunicación: permite el intercambio de información entre el medidor y la red *AMI*. Integra diferentes tecnologías de comunicación, dependiendo de la topología de la red y el entorno operativo:
    - RF (Radiofrecuencia): comunicación inalámbrica de corto o mediano alcance entre medidores y concentradores.
    - PLC (Power Line Communication): transmisión de datos a través del cableado eléctrico.
    - Ethernet o GPRS/4G: conexión directa al sistema de gestión central o concentrador de datos mediante red cableada o celular.
    - Puerto óptico o RS-485: interfaz local para lectura técnica y configuración, definida por la norma IEC 62056–21 [84].
- Medio de comunicación: representa el canal físico o lógico utilizado para la transmisión de información entre el medidor y los sistemas superiores de *AMI*, incluyendo concentradores, sistemas *HES* o plataformas de gestión de datos de medición (MDM).

Figura 3.3: Componentes del medidor inteligente



Fuente: Tomado de [85]

3.4 Plataformas de unidad de medida basadas en DLMS/COSEM

En el Laboratorio de Inteligencia Computacional de la Universidad del Valle se dispone de dos plataformas experimentales, las cuales permiten realizar pruebas de comunicación y seguridad sobre medidores que emplean distintos protocolos de transmisión en las capas bajas del modelo OSI. Aunque cada plataforma utiliza una tecnología de comunicación diferente, ambas comparten una misma capa de aplicación basada en el protocolo *DLMS/COSEM*. La primera plataforma está conformada por medidores inteligentes de la marca **Star** (**Figura 3.4a**), los cuales utilizan el protocolo **G3-PLC** para la transmisión de datos sobre la red eléctrica. La segunda plataforma emplea medidores de la marca **Circuitor** (**Figura 3.4b**), cuya comunicación se basa en el protocolo **PRIME** (*Powerline Intelligent Metering Evolution*). En ambos casos, los dispositivos implementan DLMS/COSEM como protocolo de aplicación, lo que les permite utilizar una estructura común, modelos de autenticación y mecanismos de seguridad definidos en la norma IEC 62056 [86].

A diferencia de una infraestructura *AMI* completa, estas plataformas no incorporan *UC*, *HES* ni módulos *MDM*. Su función principal es servir como entorno de ensayo controlado para estudiar el comportamiento ante ataques de *Denegación de servicios (DoS)* en la unidad de medida.

Figura 3.4: Plataformas de unidad de medida



(a) Medidor Start DTS27



(b) Medidor Circuitor 410-ZD1B-B0B-12

3.4.1 Características técnicas de los protocolos PLC utilizados

El protocolo G3-PLC (Power Line Communication) utiliza modulación OFDM y soporte para IPv6 mediante 6LoWPAN, lo que le permite una alta eficiencia en redes eléctricas con ruido o atenuación. Proporciona mecanismos de seguridad en la capa MAC basados en cifrado AES-128/CCM y autenticación de tramas, con opciones de gestión de claves mediante *Logical Bootstrap Security* (LBS) o servidores AAA (*Authentication, Authorization and Accounting*) [87, 86].

Por su parte, el protocolo PRIME define su propio estándar PLC para las capas física y de enlace, también con modulación OFDM, y utiliza una topología jerárquica de tipo árbol (nodo base y nodos de servicio). Dispone de tres perfiles de seguridad (0, 1 y 2), donde el perfil 2 incluye cifrado AES-128 y autenticación de tramas, proporcionando el mayor nivel de protección a nivel MAC, al igual que G3-PLC, se integra con *DLMS/COSEM* en la capa de aplicación, lo que permite uniformar la estructura de comunicación y los servicios de intercambio de datos [88, 86]. La **Tabla 3.1** resume las principales características de las dos plataformas de unidad de medida.

3.5 Protocolo DLMS/COSEM

El protocolo *DLMS (Device Language Message Specification)* y su complemento *COSEM (Companion Specification for Energy Metering)* constituyen el estándar internacional de comunicación más utilizado en los sistemas *AMI*. Este protocolo opera en la capa de aplicación del modelo OSI y está diseñado para el intercambio bidireccional y estandarizado de datos entre medidores inteligentes y sistemas de gestión. Su propósito principal es facilitar la lectura remota de medidas, el control de dispositivos de medición y la prestación de servicios de valor agregado en la medición de distintos tipos de energía, tales como electricidad, gas, agua o calor [89, 90].

Tabla 3.1: Fichas técnicas de las plataformas de unidad de medida basadas en DLMS/COSEM.

Aspecto	Plataforma 1: G3-PLC (Star)	Plataforma 2: PRIME (Circuitor)
Tipo de plataforma	Unidad de medida inteligente con comunicación PLC G3-PLC.	Unidad de medida inteligente con comunicación PLC PRIME.
Modelo / fabricante	Medidor Star (equipo experimental del Laboratorio de Inteligencia Computacional).	Medidor Circuitor (equipo experimental del Laboratorio de Inteligencia Computacional).
Capa física / enlace	Protocolo G3-PLC basado en modulación OFDM, soporte 6LoWPAN e IPv6; operación en bandas CENELEC A.	Protocolo PRIME PLC con modulación OFDM, topología jerárquica (nodo base y nodos servicio) y operación en bandas CENELEC A.
Capa de aplicación	DLMS/COSEM conforme a la IEC 62056.	DLMS/COSEM conforme a la IEC 62056.
Mecanismos de seguridad	Cifrado AES-128/CCM en capa MAC, autenticación mediante LBS o AAA (RADIUS).	Perfiles de seguridad 0/1/2; el perfil 2 implementa cifrado AES-128 y autenticación de tramas MAC.
Vulnerabilidades y puntos de prueba	Susceptible a ataques DoS por ruido o inyección de tramas en la capa física, y a saturación de peticiones DLMS a nivel de aplicación. Se recomienda validar la gestión de claves y autenticación mutua HLS.	Riesgos asociados a saturación del canal PLC y ataques durante el registro de nodos o repetición de tramas. Se recomienda uso del perfil 2 y verificación de unicidad de contadores DLMS.
Aplicaciones de prueba recomendadas	Ensayos de resiliencia frente a interferencia PLC, flooding de tramas MAC, y saturación de servicios GET/SET del protocolo DLMS/COSEM.	Ensayos sobre manejo de eventos simultáneos, saturación del canal PLC y validación de autenticación DLMS en sesiones concurrentes.
Observaciones generales	Alta robustez frente a ruido eléctrico; adecuada para entornos densos con topología mesh. Requiere configuración cuidadosa de autenticación LBS.	Ampliamente adoptada en Europa; adecuada para topologías jerárquicas. Se recomienda emplear el perfil de seguridad 2 y cifrado AES-128.

Desarrollado en 1997 y adoptado por la *International Electrotechnical Commission (IEC)* como la serie de normas *IEC 62056*, este protocolo ha sido implementado por un gran número de fabricantes y proveedores de servicios eléctricos, convirtiéndose en uno de los estándares más extendidos en el ámbito de la medición inteligente [91, 92]. Su adopción generalizada se debe a su capacidad de interoperabilidad, escalabilidad y compatibilidad con diferentes medios de comunicación y arquitecturas de red [89]. El estándar *DLMS/COSEM* combina dos componentes fundamentales. Por un lado, **DLMS** define la especificación del lenguaje de mensajes y los servicios de aplicación necesarios para establecer la comunicación y acceder a los objetos de medición. Por otro lado, **COSEM** provee el modelo de interfaz orientado a objetos, que permite representar los diferentes elementos funcionales del sistema de medición de manera estructurada. Este modelo organiza los dispositivos en una jerarquía lógica: cada dispositivo físico (como un medidor) contiene uno o más dispositivos lógicos, y cada dispositivo lógico incluye un conjunto de *objetos COSEM*, los cuales representan parámetros, medidas, configuraciones o acciones ejecutables [91]. Cada objeto COSEM es una instancia de una *Clase de Interfaz (CI)* definida en el *Libro Azul* de la especificación, donde se establecen los atributos y métodos disponibles para cada tipo de objeto. Estas clases funcionan de manera análoga a las interfaces de la programación orientada a objetos, lo que permite modelar funcionalidades específicas de los medidores. La identificación de estos objetos se realiza mediante el sistema *OBIS*, que asigna un código único de seis bytes encargado de clasificar y nombrar cada parámetro de medición [92].

El modelo de comunicación de *DLMS/COSEM* sigue una arquitectura **cliente-servidor**. En

este esquema, los medidores inteligentes actúan como servidores que responden a las solicitudes de clientes, tales como los sistemas de cabecera *Head End System (HES)* o las unidades concentradoras de datos. Los servicios principales definidos por el protocolo son GET, SET y ACTION, los cuales permiten leer, escribir o ejecutar métodos sobre los objetos COSEM respectivamente [90, 91].

3.5.1 Estructura y documentación del protocolo DLMS/COSEM

En su estructura interna, la capa de aplicación del protocolo *DLMS/COSEM* está compuesta por el Objeto de Servicio de Aplicación (ASO, Application Service Object), encargado de gestionar la comunicación entre los procesos de aplicación dentro del modelo cliente-servidor. Este componente constituye el núcleo funcional de la capa de aplicación y asegura que los intercambios de información entre los dispositivos de medición y los sistemas de gestión se realicen de forma ordenada y segura [90, 89]. El ASO incluye tres elementos esenciales:

1. Elemento de Servicio de Control de Asociación (ACSE, Association Control Service Element), responsable del establecimiento, mantenimiento y liberación de asociaciones entre el cliente y el servidor.
2. Elemento de Servicio de Aplicación DLMS Extendido (xDLMS ASE, Extended DLMS Application Service Element), encargado del transporte de datos entre las aplicaciones *COSEM*, garantizando la correcta ejecución de los servicios GET *Lectura de atributos*, SET *Escritura de atributos* y ACTION *Ejecución de métodos*.
3. Función de Control (CF, Control Function), que coordina la interacción y sincronización entre los componentes anteriores dentro del intercambio de mensajes.

De forma complementaria, la especificación contempla la existencia de un mapeador opcional de Nombres Cortos (SN Mapper), utilizado principalmente en entornos donde los recursos de comunicación son limitados. Este componente permite traducir los *Nombres Lógicos (LN)* definidos por los códigos *OBIS* a identificadores numéricos cortos, reduciendo la carga de procesamiento y el tamaño de los mensajes transmitidos [91, 92]. Toda la documentación técnica del protocolo *DLMS/COSEM* se encuentra estructurada en los denominados *Colored Books* y su traducción *Libros Coloreados*, mantenidos por la *DLMS User Association (DLMS UA)*, los cuales establecen las normas y procedimientos para su implementación y certificación [89, 90]:

- El Libro Azul define el modelo de objetos *COSEM*, el sistema de identificación *OBIS* y las clases de interfaz que describen las funciones de los medidores.
- El Libro Verde describe la arquitectura del protocolo, su estructura de capas y los mecanismos de comunicación soportados.
- El Libro Amarillo especifica las pruebas de conformidad y los procedimientos necesarios para la certificación de los dispositivos.

- El Libro Blanco recopila el glosario de términos, definiciones y conceptos clave relacionados con el estándar.

Una vez que un dispositivo supera las pruebas de conformidad definidas en el *Libro Amarillo*, la *DLMS User Association* emite un certificado oficial de conformidad *DLMS/COSEM*, el cual garantiza su interoperabilidad con otros equipos y sistemas certificados a nivel internacional [92, 89]. Este proceso de validación asegura la consistencia técnica, la compatibilidad y la seguridad en la implementación del protocolo dentro de las *Advanced Metering Infraestructure (AMI)*.

3.5.2 Sistema de Identificación OBIS

El *Sistema de Identificación de Objetos (OBIS)* constituye el mecanismo de identificación estandarizado empleado en el protocolo *DLMS/COSEM* para clasificar, localizar y acceder de manera inequívoca a los datos y parámetros almacenados en un medidor inteligente. Cada código *OBIS* actúa como un identificador único que permite relacionar los objetos definidos en el modelo *COSEM* con sus valores reales de medición o con la información de configuración correspondiente. En términos funcionales, el sistema *OBIS* se utiliza para identificar:

- Los nombres lógicos (LN) de los objetos definidos en el modelo *COSEM*.
- Los valores visibles en la interfaz del medidor, es decir, aquellos datos que se muestran en la pantalla local del dispositivo.
- Los valores transmitidos a través de los canales de comunicación, empleados para la lectura remota o la gestión de datos en los sistemas de supervisión.

La estructura de un código *OBIS* está compuesta por seis campos alfanuméricos, designados convencionalmente como *A–B–C–D–E–F*, donde cada campo representa un byte con un valor comprendido entre 0 y 255. Estos seis grupos definen de manera jerárquica la naturaleza, origen y destino de la información dentro del medidor [84]. Gracias a esta codificación, cada objeto *COSEM* dentro del medidor puede ser referenciado de forma única y estandarizada, facilitando la interoperabilidad entre diferentes fabricantes y sistemas de gestión.

Tabla 3.2: Descripción de los campos del código OBIS según la norma IEC 62056–61 [84].

Campo	Descripción según IEC 62056–61
A	Indica el tipo de medio o portador de energía al que pertenece el objeto (por ejemplo, electricidad, gas, calor, agua o sistemas de información). Este campo permite diferenciar entre los distintos dominios de medición.
B	Identifica el canal o punto de medición asociado. En el caso de un medidor con varios canales de entrada o salida, este valor distingue cada uno de ellos.
C	Define la magnitud física o abstracta que el objeto representa, como corriente, tensión, potencia activa, potencia reactiva, frecuencia, volumen, temperatura, entre otras.
D	Especifica el tipo de valor registrado o el resultado del procesamiento de la magnitud medida (por ejemplo, valor instantáneo, máximo, mínimo, acumulado o calculado).

Continúa en la siguiente página

Tabla 3.2 – Continua de la página anterior

Campo	Descripción según IEC 62056–61
E	Proporciona información adicional relacionada con el modo de medición o la tarifa aplicada. Se utiliza para distinguir valores de medición asociados a distintas tarifas, períodos o modos operativos.
F	Indica el número de almacenamiento o índice de facturación, asociado al período de registro o a la estructura temporal de los datos almacenados. Si no aplica, se asigna el valor 255.

En conjunto, los seis campos que conforman la estructura del código *OBIS* permiten describir de forma precisa y estandarizada cualquier objeto de medición dentro de un sistema basado en el protocolo *DLMS/COSEM*. Mientras la **Tabla 3.2** detalla la función general de cada campo (A–F), la segunda **Tabla 3.3** ejemplifica la codificación específica del campo A, encargado de identificar el medio o tipo de energía al que pertenece el objeto. Esta sistematización posibilita que los medidores inteligentes y los sistemas de gestión interpreten de manera uniforme los datos de distintos fabricantes, garantizando la interoperabilidad, la trazabilidad y la consistencia semántica de la información medida según la norma *IEC 62056–61*.

Tabla 3.3: Valores del campo A del código OBIS conforme a la norma IEC 62056–61 [84].

Código (A)	Definición según IEC 62056–61
0	Objetos abstractos o de aplicación general que no pertenecen a un medio de energía específico.
1	Objetos relacionados con electricidad (energía eléctrica y magnitudes derivadas).
4	Objetos asociados a la distribución o asignación de costes energéticos.
5	Objetos utilizados para la medición de energía o magnitudes de frío.
6	Objetos utilizados para la medición de energía o magnitudes de calor.
7	Objetos correspondientes al medio gas y sus magnitudes asociadas.
8	Objetos correspondientes al medio agua fría.
9	Objetos correspondientes al medio agua caliente.
Cualquier otro	Valor reservado para futuras extensiones o medios de energía no definidos.

3.5.3 Seguridad, autenticación y control de acceso en DLMS/COSEM

El protocolo *DLMS/COSEM* implementa un modelo de seguridad integral que combina autenticación, control de acceso y protección criptográfica para garantizar la integridad y confidencialidad de la comunicación entre los medidores inteligentes (servidores) y los sistemas de gestión o concentradores (clientes). Durante la fase de establecimiento de la *Asociación de Aplicaciones (AA)*, se definen distintos niveles de autenticación que determinan el grado de confianza y robustez del enlace entre ambas partes [93].

El estándar contempla tres niveles de autenticación. El primero, denominado *Lowest Level Security*, no incluye verificación de identidad y solo permite el acceso a información básica o pública del medidor; su uso se restringe a entornos de prueba o configuraciones locales. El segundo, *Low Level Security (LLS)*, requiere que el cliente se autentique frente al servidor mediante una

contraseña transmitida en texto plano. Aunque introduce una capa mínima de protección, este método sigue siendo vulnerable a ataques de interceptación o fuerza bruta, por lo que solo se recomienda cuando el canal de comunicación es físicamente seguro o cuenta con cifrado adicional. El tercer nivel, *High Level Security (HLS)*, es el más robusto y recomendado por la *DLMS User Association (DLMS UA)* [94]. Implementa autenticación mutua entre cliente y servidor mediante un proceso de intercambio de retos y respuestas *(challenge–response)*, que permite verificar la identidad de ambas partes sin revelar las claves secretas y proteger frente a ataques de repetición o suplantación de identidad.

Dentro del nivel HLS se incluyen distintos métodos de autenticación: HLS-MD5, HLS-SHA1, HLS-GMAC, HLS-SHA256 y HLS-ECDSA. Las versiones basadas en MD5 y SHA1 han quedado obsoletas debido a sus vulnerabilidades ante ataques de colisión, mientras que HLS-ECDSA (método 5) ofrece el mayor nivel de seguridad al utilizar firmas digitales basadas en criptografía de curvas elípticas (ECC) dentro de una Infraestructura de Clave Pública (PKI), vinculando de forma segura las identidades de los dispositivos con sus claves criptográficas[94]. Además de la autenticación, *DLMS/COSEM* define un sistema de control de acceso jerárquico, que regula los permisos de lectura, escritura o ejecución sobre los objetos COSEM. Estos permisos, denominados *Access Rights*, dependen del rol del usuario y del nivel de autenticación alcanzado. De esta manera, el sistema restringe automáticamente cualquier intento de acceso no autorizado.

En materia criptográfica, el protocolo establece un esquema de protección avanzado destinado a preservar la confidencialidad, integridad y autenticidad de los datos transmitidos. Cada medidor inteligente dispone de tres claves principales que intervienen en este proceso [94]:

- Clave maestra, una clave AES programada en el firmware durante la fabricación del medidor, utilizada para cambiar el método de cifrado y actualizar las claves internas.
- Clave de cifrado, de 128 o 256 bits, responsable de proteger los mensajes intercambiados entre los dispositivos.
- Clave de autenticación, del mismo tamaño que la de cifrado, empleada para generar una etiqueta o tag de autenticación que garantiza la integridad de cada mensaje y demuestra el conocimiento legítimo de la clave compartida.

El protocolo admite tres modos de comunicación: en texto plano (sin cifrado), cifrado mediante una clave global compartida por todos los dispositivos de la red, o cifrado mediante una clave dedicada de sesión, que se genera dinámicamente para cada intercambio. Este último modo es el más seguro, pues impide que una clave comprometida afecte futuras sesiones.

DLMS/COSEM utiliza el algoritmo AES en modo *Galois Counter Mode* (GCM), que combina cifrado y autenticación en una sola operación. Este modo emplea una clave AES de 128 bits junto

con un vector de inicialización (IV) único y un contador de bloque de 32 bits que comienza en 1. La generación del flujo de cifrado (*keystream*) se realiza aplicando la función AES a la concatenación del IV con el contador correspondiente. La unicidad del IV es fundamental si se repitiera, un atacante podría reconstruir el flujo de claves y comprometer la confidencialidad de los datos.

Para evitarlo, *DLMS/COSEM* garantiza un IV único concatenando dos valores: el *AP Title*, un identificador único de 64 bits que distingue a cada dispositivo dentro de la red, y el *Frame Counter*, un contador de 32 bits que se incrementa con cada mensaje enviado. De esta manera, se obtiene un IV de 96 bits, considerado seguro según las recomendaciones del estándar AES-GCM [94]. Durante el proceso de cifrado, el primer bloque del keystream se reserva para proteger el tag de autenticación, mientras que los bloques siguientes se utilizan para cifrar el contenido del mensaje. Si la longitud del mensaje no coincide con el tamaño de bloque (128 bits), se añade un pequeño relleno (padding) al final para completar la estructura. Este mecanismo garantiza que cada mensaje se cifre de manera única, íntegra y verificable.

3.6 Vulnerabilidades del protocolo DLMS/COSEM

Las fuentes consultadas distinguen dos grandes familias de vulnerabilidades: (A) las que derivan de decisiones o limitaciones en la propia especificación del protocolo *DLMS/COSEM*, y (B) las que emergen por errores o malas prácticas en las implementaciones de fabricantes u operadores. Para evaluar la seguridad de la unidad de medida conviene tratarlas por separado, porque las contramedidas son distintas: unas requieren actualizar normas o cambiar parámetros de la especificación; otras se corrigen con buenas prácticas de desarrollo y configuración [86].

3.6.1 Vulnerabilidades inherentes al protocolo

Estas fallas nacen en la definición del estándar y afectan a cualquier equipo que lo implemente, salvo que se hayan introducido restricciones adicionales [92, 91]:

- Posibilidad de degradación de la autenticación (Authentication Downgrade): *DLMS/COSEM* permite que la autenticación sea opcional y no necesariamente vinculada al cifrado de los mensajes. Un atacante con capacidad de interceptar o modificar el flujo puede manipular el byte de seguridad presente en el encabezado (transmitido en texto claro) o truncar la APDU para eliminar el *tag* de autenticación. Esto permite que mensajes que deberían estar protegidos sean aceptados como válidos, reduciendo efectivamente el nivel de seguridad.
- Fuga de información por metadatos en claro: Aunque el contenido (*payload*) se encuentre cifrado, ciertos campos del encabezado como la etiqueta que identifica el tipo de APDU o el modo de comunicación permanecen visibles en texto claro. Esto permite a un observador inferir cuándo se envían solicitudes del tipo *GET* o *ACTION*, e incluso aprovechar el tamaño fijo de algunas tramas para realizar ataques de análisis de tráfico o de texto plano conocido

(*known-plaintext attacks*).

- Debilidades en los métodos HLS (High Level Security): Algunos mecanismos de autenticación HLS antiguos, como HLS-MD5 y HLS-SHA1, presentan vulnerabilidades criptográficas conocidas y no deben emplearse. Otros métodos más robustos, como HLS-SHA256, pueden verse comprometidos si los secretos utilizados tienen baja entropía, dado que todos los parámetros del hash son públicos. Esto permite ataques de fuerza bruta *offline* contra secretos débiles. Además, cuando múltiples clientes comparten el mismo secreto HLS, se posibilitan ataques de suplantación o de sesión paralela.
- Permiso para el uso de algoritmos obsoletos o modos débiles: La especificación *DLMS/COSEM* aún permite la utilización de algoritmos y parámetros criptográficos considerados inseguros por estándares actuales. En particular, el uso de *Low Level Security* (LLS) se basa en esquemas de autenticación simples, generalmente mediante contraseñas estáticas que pueden transmitirse en texto plano, lo que las hace susceptibles a ataques de interceptación y acceso no autorizado. Por otro lado, aunque *High Level Security* (HLS) introduce mecanismos más robustos basados en criptografía, su seguridad depende en gran medida de una correcta configuración. Implementaciones deficientes, como el uso de claves débiles, pueden derivar en ataques de degradación de seguridad (*downgrade attacks*).
- Riesgos asociados al modo GCM con *tags* cortos: Cuando se utiliza el modo AES-GCM (*Galois/Counter Mode*) con etiquetas de autenticación demasiado cortas, aumenta la probabilidad de falsificación de mensajes. Una falsificación exitosa puede revelar información sobre la clave de autenticación, comprometiendo tanto la integridad como la confidencialidad de la comunicación.

3.6.2 Vulnerabilidades de implementación (errores operativos y de desarrollo)

Aunque la especificación *DLMS/COSEM* es sólida desde el punto de vista conceptual, muchas incidencias de seguridad observadas en entornos reales son de prácticas de configuración o de errores de desarrollo que degradan el nivel de protección efectivo de los dispositivos. Estas vulnerabilidades no dependen del protocolo en sí, sino de su implementación y despliegue [86, 92, 90].

- Uso de LLS (Low Level Security): El modo de autenticación LLS transmite las contraseñas en texto plano, lo que lo hace completamente vulnerable frente a ataques de interceptación pasiva o *Man-In-The-Middle*. Su uso debe restringirse a entornos de laboratorio o canales físicamente seguros, y estar prohibido en entornos operativos.
- Contador de trama no reforzado (*Frame Counter*): Si el servidor acepta mensajes cifrados cuyo contador de trama es menor o igual al último valor recibido, el sistema queda expuesto a ataques de repetición (*replay attacks*). Este contador debe ser estrictamente monotónico y el servidor debe rechazar cualquier mensaje con un valor no superior al registrado.
- Aceptación de AP Titles idénticos o arbitrarios: Permitir comunicaciones entre dispositivos que comparten el mismo AP Title incrementa el riesgo de suplantación de identidad. Si

además se aceptan AP Titles arbitrarios, un atacante podría abrir múltiples conexiones con identificadores falsos para agotar los recursos del dispositivo o reutilizar contadores de invocación (*Invocation Counters*) y ejecutar ataques de repetición.

- Procesamiento de mensajes cifrados sin verificar autenticación: Algunos servidores procesan mensajes basándose únicamente en el encabezado, sin validar el *tag* de autenticación. Este comportamiento permite que un atacante inyecte comandos o manipule el contenido del mensaje mediante técnicas como *bit-flipping* o *message replacement*.
- AARQ en texto plano que provoca AARE cifrado (fuga de *keystream*): Si un servidor responde a una solicitud AARQ (Application Association Request, mensaje de solicitud de asociación entre cliente y servidor) enviada en texto plano con una respuesta AARE (Application Association Response, mensaje de respuesta a la solicitud de asociación) cifrada, el atacante podría inferir parte del *keystream* utilizado, lo que facilitaría la generación de mensajes cifrados sin conocer la clave secreta.
- Permitir ataques de diccionario en línea (*online dictionary attacks*): No establecer límites en los intentos de autenticación ni aplicar retardos progresivos facilita ataques de fuerza bruta en línea. Además, los mensajes de error diferenciados entre intentos válidos e inválidos proporcionan información adicional al atacante sobre el estado de la autenticación.

3.7 Técnicas para la implementación de las pruebas

La propuesta para la prueba establece el procedimiento técnico mediante el cual se aplicarán, en un entorno controlado, un conjunto de técnicas provenientes del dominio de la ciberseguridad, adaptadas al funcionamiento de los medidores *AMI* y al protocolo DLMS/COSEM. Esta fase actúa como el enlace entre la caracterización previa del sistema *AMI* y la generación de estímulos deliberados sobre el medidor bajo condiciones de tráfico no habituales, sin emitir interpretaciones sobre su desempeño ni realizar evaluaciones formales.

Las técnicas seleccionadas corresponden a métodos utilizados de forma tradicional en ciberseguridad ofensiva, pero reinterpretados según las restricciones operativas de los medidores inteligentes. La arquitectura *AMI*, el canal físico disponible y el modelo secuencial del intercambio DLMS/COSEM limitan los tipos de estímulos que pueden aplicarse al dispositivo. Por lo tanto, se incluyen únicamente técnicas que pueden reproducirse de manera consistente con el mecanismo de sesión, el flujo estricto petición–respuesta y las capacidades reales del medidor. La propuesta para la prueba se define a partir del esquema metodológico general que integra las etapas conceptuales y técnicas del estudio. Esta fase se encuentra representada en el **Anexo 5.1** y de manera segmentada en el **Anexo 5.2**, específicamente en la sección identificada como **A-B1**. En esta etapa se establecen las técnicas de ciberseguridad seleccionadas para las pruebas del medidor inteligente, así como los perfiles de acceso utilizados durante la prueba.

3.8 Técnicas aplicadas para la implementación de las pruebas en el medidor STAR

3.8.1 Opción 1: Fuzzing con perfil de escritura adaptado a DLMS/COSEM

La técnica de *fuzzing* implementada en esta opción se basa en la generación de cargas útiles (*payloads*) no habituales, con variación controlada de tamaño y contenido, que son inyectadas mediante operaciones de escritura DLMS/COSEM (*SET*) sobre un objeto COSEM específico. El enfoque se ejecuta bajo un perfil de escritura previamente configurado, lo cual habilita el acceso al atributo objetivo dentro del modelo de seguridad y autenticación del medidor. El script se estructura en cuatro bloques funcionales: (i) configuración y establecimiento de sesión DLMS, (ii) preparación del objeto objetivo y su tipo de dato, (iii) generación iterativa de *payloads* con múltiples estrategias, y (iv) manejo de eventos y recuperación ante interrupciones de comunicación.

3.8.1.1 Inicialización de sesión y perfil de comunicación

El script carga el perfil `escritura(settings)`, el cual define los parámetros necesarios para operar en modo escritura (por ejemplo: interfaz, autenticación, llaves o niveles de acceso, según la configuración del laboratorio). Posteriormente se instancia `GXDLMSReader` y se ejecuta la secuencia de establecimiento de sesión: apertura del medio (`media.open()`), inicialización de conexión (`initializeConnection()`) y obtención de la vista de asociación (`getAssociationView()`), garantizando que el intercambio DLMS/COSEM se encuentra activo antes de iniciar los estímulos.

3.8.1.2 Objeto y control sintáctico mínimo

El objeto bajo prueba se define mediante el código OBIS `0.0.96.1.1.255`. Para asegurar consistencia sintáctica mínima en el atributo escrito, el script fija explícitamente el tipo de dato del atributo 2 como *OCTET_STRING* (`setDataType(2, DataType.OCTET_STRING)`). Esto permite que los *payloads* generados alcancen el procesamiento de la capa de aplicación DLMS/COSEM, reduciendo el sesgo por rechazos triviales derivados de tipos incompatibles.

3.8.1.3 Generación de payloads y ejecución indefinida

La prueba se ejecuta en un bucle indefinido (`while True`), donde cada iteración incrementa un contador y construye un *payload* cuyo tamaño crece de manera cíclica según la expresión `(step % MAX_PAYLOAD_SIZE) + 1`. Con ello, el script introduce variación sistemática del tamaño hasta un máximo configurado (`MAX_PAYLOAD_SIZE`), evitando un crecimiento ilimitado que comprometa los recursos del equipo ejecutor. La generación de datos se realiza mediante estrategias alternadas que cubren diferentes clases de contenido: caracteres imprimibles codificados en UTF-8, rellenos nulos, patrones repetitivos, secuencias asociadas a cadenas

formateadas y bytes aleatorios criptográficamente (`os.urandom`). En cada iteración se ejecuta la escritura (`write(obj,2)`) y una lectura inmediata (`read(obj,2)`) como verificación funcional del canal de intercambio, sin que ello implique evaluación del desempeño del dispositivo.

El script registra excepciones como *eventos detectados* y contempla la posibilidad de interrupciones de comunicación o reinicio del medidor. Cuando se identifica un error de comunicación o el medio no se encuentra abierto, se aplica una espera controlada y se intenta reestablecer la sesión (cierre/apertura del medio e inicialización de conexión). Esta lógica de recuperación permite sostener pruebas de larga duración y observar patrones de indisponibilidad lógica del servicio DLMS/COSEM bajo estímulos repetitivos.

3.8.2 Flujo de ejecución del script de fuzzing

El flujo de ejecución del script se desarrolla de manera secuencial bajo el modelo petición–respuesta de DLMS/COSEM, con un ciclo indefinido de generación y envío de estímulos:

1. Cargar el perfil de escritura y configurar el cliente DLMS/COSEM.
2. Abrir el medio de comunicación y establecer la sesión DLMS:
   a) Inicializar conexión (`initializeConnection`).
   b) Obtener la vista de asociación (`getAssociationView`).
3. Definir el objeto objetivo (`GXDLMSData`) con OBIS `0.0.96.1.1.255`.
4. Fijar el tipo del atributo 2 como *OCTET_STRING*.
5. Iniciar bucle indefinido:
   a) Incrementar contador de iteración.
   b) Calcular tamaño del *payload* con crecimiento cíclico hasta `MAX_PAYLOAD_SIZE`.
   c) Generar *payload* mediante una estrategia aleatoria.
   d) Asignar el *payload* al atributo 2 y enviar *SET* (`write`).
   e) Ejecutar una lectura inmediata (`read`) como verificación funcional del intercambio.
   f) Si ocurre evento de comunicación o cierre del medio, esperar y reintentar reconexión.
   g) Continuar con la siguiente iteración hasta detención manual.
6. Al finalizar, cerrar sesión y liberar recursos.

La **Tabla 3.4** presenta la clasificación de las familias de estímulos de *fuzzing* implementadas durante la prueba, organizadas según el tipo de carga generada, el objeto COSEM y la mutación aplicada sobre el atributo seleccionado. Esta clasificación permite estructurar los distintos patrones de entrada no habituales introducidos en el medidor.

ID	Estrategia de fuzzing	Objeto (OBIS)	Atributo	Mutación aplicada
FZ2-01	Cadenas ASCII imprimibles	0.0.96.1.1.255	2	Generación de caracteres UTF-8 imprimibles con longitud variable entre 1 y MAX_PAYLOAD_SIZE
FZ2-02	Relleno con bytes nulos	0.0.96.1.1.255	2	Secuencias repetitivas de bytes `0x00` con longitud variable
FZ2-03	Patrones repetitivos	0.0.96.1.1.255	2	Repetición de un mismo carácter ASCII para distintos tamaños de carga
FZ2-04	Secuencias formateadas	0.0.96.1.1.255	2	Inyección de patrones asociados a cadenas de formato (`%s`, `%n`, `%x`, `%d`)
FZ2-05	Datos binarios aleatorios	0.0.96.1.1.255	2	Generación de secuencias binarias pseudoaleatorias mediante `os.urandom()`

Tabla 3.4: Clasificación de las familias de estímulos de fuzzing aplicadas sobre el objeto COSEM seleccionado, manteniendo coherencia sintáctica con el tipo de dato configurado.

3.8.3 Opción 2: Flooding de lectura (stress) con perfil de lectura

Esta opción implementa una técnica de *flooding* basada en lectura intensiva sobre un objeto *Profile Generic* (perfil de carga) mediante el envío repetitivo de solicitudes DLMS/COSEM válidas bajo un perfil de lectura. A diferencia de enfoques orientados a escritura, el objetivo aquí es incrementar la presión lógica sobre el medidor solicitando bloques de datos históricos en volumen elevado y sostenida, lo que obliga al dispositivo a procesar y transferir múltiples registros bajo el modelo secuencial de petición–respuesta.

El script opera sobre el OBIS `1.0.99.1.0.255`, correspondiente a un *Load Profile*, y utiliza solicitudes de lectura por rangos de entradas con una cantidad elevada de registros por petición (`ENTRIES_TO_REQUEST`). Esta configuración busca provocar condiciones de carga asociadas a transferencia segmentada y manejo intensivo de buffers, manteniendo el intercambio dentro de las operaciones permitidas por DLMS/COSEM.

3.8.3.1 Arquitectura del script

El script se estructura en cuatro bloques funcionales:

- Inicialización de perfil y sesión DLMS: se carga el perfil `lectura(settings)` y se establece la sesión DLMS/COSEM mediante apertura del medio, inicialización de conexión y asociación.

- Preparación del objeto: se instancia el objeto `GXDLMSProfileGeneric` con el OBIS del perfil de carga y se realiza una lectura inicial para confirmar su disponibilidad y obtener el número de entradas en uso (`entriesInUse`).

- Generación de tráfico por lectura masiva: en un bucle indefinido, el script ejecuta solicitudes repetitivas de lectura de filas por rango de entradas, utilizando `readRowsByEntry(pg, 1, ENTRIES_TO_REQUEST)` para solicitar un número elevado de registros desde el inicio del perfil. Entre iteraciones se aplica un retardo mínimo (`WAIT_BETWEEN_REQUESTS`), con el propósito de mantener la cadencia alta.
- Gestión de eventos y recuperación: ante excepciones de comunicación o *timeout*, el script aplica una pausa controlada y reintenta la reconexión cerrando y reabriendo el medio, seguida de una reinicialización de la sesión DLMS. Esto permite sostener pruebas prolongadas y registrar interrupciones del canal de comunicación.

3.8.3.2 Flujo de ejecución del flooding de lectura

El flujo de ejecución del script se describe como sigue:

1. Cargar el perfil de lectura y configurar los parámetros del cliente DLMS/COSEM.
2. Abrir el medio de comunicación e inicializar la sesión DLMS (asociación).
3. Instanciar el objeto *Profile Generic* mediante el OBIS `1.0.99.1.0.255`.
4. Leer atributos base del objeto para verificar su existencia y consultar el número de entradas en uso.
5. Iniciar un ciclo indefinido de *stress*:
   a) Solicitar un rango de registros mediante `readRowsByEntry`, desde la primera entrada hasta `ENTRIES_TO_REQUEST`.
   b) Medir el tiempo transcurrido de la operación de lectura y registrar la cantidad de filas recibidas.
   c) Ante errores de comunicación o *timeout*, aplicar espera controlada y reintentar reconexión e inicialización de sesión.
   d) Esperar `WAIT_BETWEEN_REQUESTS` antes de la siguiente iteración.
6. Finalizar por detención manual y liberar recursos cerrando la sesión.

La Tabla 3.5 resume las familias de estímulos definidas para la técnica de flooding basada en lectura, diferenciándolas por el tamaño del bloque de registros solicitado al objeto *Profile Generic* y por la cadencia de petición. Esta clasificación permite parametrizar la carga generada desde el cliente DLMS/COSEM y documentar de forma trazable las condiciones bajo las cuales se ejecuta el *stress* sobre el perfil de carga.

ID	Objeto	Operación DLMS	Parámetro de carga	Descripción del estímulo
FS2-01	Profile Generic (1.0.99.1.0.255)	Lectura por rango de entradas	50–100 registros	Solicitud repetitiva de un bloque moderado de filas por iteración
FS2-02	Profile Generic (1.0.99.1.0.255)	Lectura por rango de entradas	200–300 registros	Solicitud repetitiva de bloques grandes con retardo mínimo entre peticiones
FS2-03	Profile Generic (1.0.99.1.0.255)	Lectura por rango de entradas	500 registros (configuración base)	Lectura masiva sostenida para forzar procesamiento intensivo y transferencia segmentada
FS2-04	Profile Generic (1.0.99.1.0.255)	Lectura por rango de entradas	$\geq$500 registros	Lectura masiva prolongada ajustando el tamaño del bloque y la cadencia para incrementar presión temporal

Tabla 3.5: Clasificación de familias de estímulos para flooding de lectura sobre el perfil de carga.

3.8.4 Opción 3: Flooding de lectura en perfil (sin autenticación)

Esta opción implementa una técnica de *flooding* basada en lecturas DLMS/COSEM bajo el *perfil* , el cual corresponde a un modo de acceso que no requiere credenciales ni niveles de autenticación, a diferencia de los perfiles de lectura/escritura autenticados. Desde la perspectiva de ciberseguridad, este perfil es especialmente relevante porque representa el conjunto mínimo de capacidades de consulta que un actor podría ejercer cuando tiene acceso al canal local de comunicación, incluso sin disponer de contraseñas o llaves.

El objetivo técnico de esta opción es generar ráfagas sostenidas de solicitudes de lectura sobre un conjunto de objetos COSEM accesibles públicamente, manteniendo las operaciones dentro del intercambio estándar DLMS/COSEM y respetando el modelo secuencial de petición–respuesta.

3.8.4.1 Arquitectura del script

El script se en cuatro bloques funcionales:

- Configuración de sesión con perfil : se carga el perfil `público(settings)` y se establece la conexión DLMS/COSEM mediante apertura del medio y procedimiento de asociación (`initializeConnection`). Este bloque define un escenario de acceso sin autenticación.
- Definición del conjunto objetivo: se especifica una lista de códigos OBIS asociados a objetos de tipo `Data` que, bajo el perfil, son susceptibles de consulta (por ejemplo: nombre lógico del dispositivo, contadores de invocación, identificador de firmware, asignación SAP). Con el fin de evitar sobrecosto computacional dentro del ciclo de inundación, los objetos se instancian previamente y se almacenan en una lista `objects_to_flood`.
- Generación de tráfico por ráfagas: la prueba se ejecuta en un bucle indefinido. En cada iteración se realiza una lectura secuencial del atributo 2 (*Value*) de cada objeto predefinido

mediante `reader.read(obj,2)`, ejecutando la ráfaga lo más rápido posible. El tiempo total de cada ráfaga se registra como una referencia de la cadencia con la que el cliente logra completar un ciclo de lecturas.

- Tolerancia a fallos y mantenimiento de asociación: si la lectura de un objeto genera una excepción, el script continúa con el siguiente objeto para evitar la interrupción del flooding. Adicionalmente, se reejecuta periódicamente la inicialización de conexión (cada 50 iteraciones) con el fin de mantener la asociación activa y reducir la probabilidad de cierre por inactividad o inestabilidad del canal.

Este enfoque permite caracterizar el comportamiento del canal de comunicación frente a solicitudes repetitivas sin requerir credenciales, lo cual resulta pertinente para escenarios de exposición local donde un atacante obtiene acceso físico al puerto de comunicación del medidor.

3.8.4.2 Flujo de ejecución del flooding en perfil

El flujo lógico del script se describe como sigue:

1. Cargar el perfil y configurar los parámetros de comunicación DLMS/COSEM.
2. Abrir el medio de comunicación e inicializar la asociación DLMS.
3. Instanciar previamente los objetos `GXDLMSData` correspondientes a la lista de OBIS objetivo.
4. Iniciar un bucle indefinido de ráfagas de lectura:
   a) Iniciar medición temporal de la iteración.
   b) Leer secuencialmente el atributo 2 (*Value*) de cada objeto objetivo.
   c) Ignorar fallos puntuales por objeto y continuar la ráfaga.
   d) Registrar el tiempo total consumido por la ráfaga.
   e) Cada 50 iteraciones, reejecutar la inicialización de conexión para mantener la asociación activa.
5. Finalizar por detención manual y cerrar sesión y medio de comunicación.

La Tabla 3.6 organiza las familias de estímulos definidas para el flooding en perfil , diferenciándolas por el conjunto de objetos COSEM consultados y por la configuración operativa del ciclo de lectura. Esta clasificación documenta los estímulos aplicados desde el cliente DLMS/COSEM en un escenario sin autenticación.

ID	**Objetos**	**Operación DLMS**	**Configuración de la solicitud**
FP-01	1 objeto	Lectura (Value)	Lectura repetitiva sobre un único OBIS
FP-02	Lista base de 6 objetos	Lectura secuencial	Ráfagas continuas sobre todos los OBIS definidos
FP-03	Lista extendida	Lectura secuencial	Incremento del número de OBIS consultados por ráfaga
FP-04	Lista base de 6 objetos	Lectura secuencial	Reinicialización periódica cada N iteraciones

Tabla 3.6: Familias de estímulos definidas para flooding de lectura en perfil .

3.9 Requerimientos para la prueba de DoS

La ejecución de una prueba de vulnerabilidad por denegación de servicio (DoS) en medidores inteligentes requiere la definición previa de un conjunto de requerimientos técnicos que delimiten el entorno experimental y los elementos involucrados. Estos requerimientos permiten asegurar que los estímulos de ciberseguridad se generen y apliquen de manera controlada, coherente con las restricciones del protocolo DLMS/COSEM. En este contexto, se identifican los elementos fundamentales necesarios para la prueba, los cuales conforman la arquitectura básica de interacción entre el generador de tráfico, el software de comunicación y el dispositivo objetivo.

Los requerimientos para la prueba se estructuran conforme a la fase metodológica correspondiente del diagrama general presentado en el **Anexo 5.1** y detallado por secciones en el **Anexo 5.2**, identificada como **B1-B2**. En esta sección se definen los elementos técnicos necesarios para la ejecución de la prueba, incluyendo el medidor inteligente, el software de comunicación DLMS/COSEM y el equipo de cómputo que actúa como generador de tráfico.

3.9.1 Elementos para la prueba de DoS

La prueba de vulnerabilidad DoS se desarrolló utilizando un entorno de laboratorio compuesto por tres elementos principales. El primero es el equipo computacional, que sirve como plataforma de ejecución del software y como generador de tráfico para la aplicación de las técnicas de ciberseguridad. El segundo es el software de comunicación GuruX, encargado de generar y gestionar el intercambio de tramas conforme al protocolo. El tercero es el medidor inteligente, que actúa como dispositivo objetivo y procesa las solicitudes DLMS/COSEM. Estos elementos conforman el escenario técnico necesario para la ejecución controlada de la prueba.

3.9.1.1 Equipo computacional como servidor y generador de tráfico

El equipo computacional utilizado en la prueba cumple el rol de plataforma de ejecución para las técnicas de ciberseguridad aplicadas al medidor inteligente. Desde el punto de vista funcional, este equipo actúa como generador de tráfico y punto de control de las interacciones DLMS/COSEM, siendo el entorno desde el cual se ejecuta el software GuruX y se orquestan los estímulos dirigidos al dispositivo AMI bajo prueba. Aunque en el modelo lógico del protocolo DLMS/COSEM el medidor actúa como servidor y el cliente DLMS se ejecuta en el equipo computacional, en el contexto de la prueba de vulnerabilidad el PC se considera el origen de los estímulos de denegación de servicio. Por esta razón, se le asigna el rol de servidor o generador de tráfico dentro del escenario de ciberseguridad, diferenciando claramente el rol protocolar del rol funcional en la prueba.

3.9.1.2 Especificaciones técnicas del equipo

El equipo empleado corresponde con las siguientes características técnicas relevantes:

- Procesador: Intel® Core™ i7-8700 CPU @ 3.20 GHz, con seis núcleos físicos.
- Memoria RAM: 16 GB DDR4 con velocidad de 2667 MT/s.
- Sistema operativo Windowns, arquitectura de 64 bits, procesador x64.

Estas especificaciones proporcionan una capacidad de procesamiento suficiente para ejecutar múltiples hilos de forma concurrente, controlar temporizaciones de envío de tramas y mantener sesiones DLMS activas durante periodos prolongados sin degradación del sistema anfitrión.

3.9.1.3 Medidor Inteligente DTS27 de Star Instrument

El medidor DTS27 es un dispositivo electrónico trifásico tetrafilar diseñado para la medición de energía en entornos residenciales, comerciales e industriales. Fabricado por Shenzhen Star Instrument Co., Ltd., el equipo integra registro de eventos, capacidades de comunicación avanzadas y compatibilidad con infraestructuras *AMI* modernas. De acuerdo con el manual técnico del fabricante [95] y la hoja de especificaciones comerciales [96], el medidor cumple con los estándares internacionales IEC 62052-11, IEC 62053-22 y IEC 62053-23, lo que asegura interoperabilidad en aplicaciones de medición estática de energía activa y reactiva. El modelo DTS27 está diseñado para operación en sistemas de **tres fases y cuatro hilos**, según se detalla en la Tabla de Especificaciones del fabricante. El medidor soporta:

- Corriente nominal de 5 A y corriente máxima de 100 A.
- Frecuencia nominal de 50–60 Hz.
- Constante de energía de 200 imp/kWh y 200 imp/kvarh.

Estas características habilitan al DTS27 como un medidor apto para aplicaciones de alta precisión y para cumplir perfiles de carga horarios en infraestructura *AMI*. El medidor tiene capacidades de medición y diagnóstico. Según el manual técnico, registra energía activa y reactiva directa e inversa, potencia activa y aparente, demanda activa y reactiva, parámetros instantáneos (voltaje, corriente, frecuencia) y estados de fase. Entre las capacidades adicionales se encuentran:

- Registro de eventos anómalos: corriente inversa, pérdida de fase, fase inversa, neutro perdido, sobrevoltaje y sobrecorriente. Se almacenan los 10 eventos más recientes.
- Funciones de auto-diagnóstico para error de batería, error de reloj y falla de memoria.
- Display LCD de 8 dígitos con indicadores de energía, fase, batería, códigos OBIS y alarmas.

Estas funciones permiten el uso del medidor tanto para medición primaria como para análisis de condiciones operativas dentro de un sistema *AMI*. El DTS27 posee una carcasa de policarbonato estabilizado UV, bloque de terminales conforme a DIN 43857 y terminales de latón con recubrimiento de níquel para ambientes exigentes. Sus dimensiones son 287.7 mm × 204.0 mm × 83.0 mm, con un peso menor a 2 kg. Incluye:

- Puerto óptico IEC 62056-21 para comunicación local.

- Puerto RS-232 para módulos GPRS o PSTN.
- Indicadores LED para energía activa y reactiva.
- Botón de ciclo de despliegue y botón de configuración con sello.

El DTS27 implementa el protocolo DLMS/COSEM en la capa de aplicación, lo que lo hace interoperable con herramientas de lectura como GuruX. El acceso a datos se realiza mediante objetos identificados por códigos OBIS, los cuales permiten consultar energía, demanda, perfiles de carga, eventos y parámetros instantáneos. La operación DLMS del medidor es de naturaleza estrictamente secuencial, es decir, admite una sola transacción por sesión, lo cual es consistente con el diseño interno del stack y con la interfaz óptica utilizada.

3.9.1.4 GuruX

GuruX Ltd. [97] desarrolla un conjunto de componentes de software en código abierto orientados a la comunicación con medidores inteligentes basados en el estándar *DLMS/COSEM*. Su relevancia proviene de que implementa el protocolo de manera completa, abarcando el nivel de aplicación, el modelo de objetos COSEM, la construcción de tramas HDLC, los mecanismos de asociación AARQ/AARE, los niveles de seguridad del estándar y la interpretación de códigos *OBIS* para acceder a magnitudes específicas del medidor. Las librerías están disponibles para múltiples lenguajes, lo que permite integrarlas en diferentes entornos de prueba [98].

Para la construcción de esta prueba se utilizó la implementación en Java, que proporciona una abstracción clara de cada componente del estándar. La librería incluye clases para gestionar la apertura y cierre de sesiones, construir solicitudes de lectura y escritura, procesar respuestas provenientes del medidor y manipular objetos COSEM en su estructura formal. Cada clase contiene la lógica interna necesaria, incluyendo la segmentación, el control de estados, la verificación de integridad y el manejo de errores del protocolo. Esta estructura hace posible reproducir interacciones reales con el medidor sin depender de utilidades externas ni de herramientas propietarias del fabricante. La importancia de *GuruX* en el desarrollo de esta prueba radica en que permite emitir solicitudes válidas dentro del marco del estándar, garantizando que los estímulos aplicados sobre el medidor provienen de un cliente DLMS legítimo, ya que solo las solicitudes estructuradas según *DLMS/COSEM* son interpretadas por el medidor y procesadas de forma secuencial. De esta manera, las técnicas aplicadas durante la prueba se ejecutan de forma controlada y respetando las restricciones operativas del dispositivo.

La librería implementa la tabla *OBIS* completa, asociando cada identificador con la clase COSEM y los atributos correspondientes. Esto permite que la operación de lectura consista en especificar el *OBIS*, el atributo y el tipo de acceso requerido. *GuruX* genera la APDU correspondiente, encapsula la información en el framing HDLC, la envía al dispositivo y procesa la respuesta, devolviendo el valor del atributo en el tipo de dato definido por el estándar. Los

medidores AMI almacenan la mayoría de su información mediante objetos COSEM Cada uno de estos elementos posee su propio código *OBIS*, lo que permite acceder a ellos mediante un método uniforme e independiente del fabricante. La escritura de atributos sigue una lógica similar, con la diferencia de que requiere niveles de seguridad habilitados y permisos disponibles en la asociación creada. Los perfiles de carga se almacenan como tablas estructuradas donde cada fila representa un intervalo de medición y cada columna corresponde a objetos COSEM asociados al perfil. *GuruX* implementa el proceso completo para recuperar estos registros: solicita la estructura del perfil, selecciona los rangos temporales requeridos y obtiene las entradas almacenadas en la memoria del dispositivo. En cuanto a los eventos, la librería permite consultar los registros de sucesos capturados por el medidor, tales como interrupciones, reinicios, accesos, fallas internas o alteraciones detectadas por el equipo. El uso de *GuruX* permite que las técnicas aplicadas se desarrollen dentro de un marco compatible con el estándar DLMS/COSEM. La librería facilita:

- la generación repetida de solicitudes válidas con intervalos reducidos,
- la manipulación de estructuras internas del medidor mediante códigos OBIS,
- la lectura consecutiva de perfiles de carga bajo condiciones de presión temporal,
- la emisión de secuencias de tramas alteradas dentro del margen permitido por el estándar,

El repositorio oficial de GuruX en GitHub incluye utilidades adicionales para diagnóstico, como trazado de comunicación, interpretación de errores, registros de intercambio y validación del framing HDLC. Estas herramientas permiten documentar el comportamiento de las solicitudes enviadas y analizar en detalle las respuestas generadas por el medidor.

3.10 Síntesis

Este capítulo permitió definir y estructurar la metodología empleada para la realización de la prueba de vulnerabilidad ante *DoS* en la unidad de medida dentro de un sistema *AMI*. A través de la descripción de las etapas, criterios y herramientas utilizadas, se estableció un proceso ordenado que orienta la preparación del entorno de prueba, la ejecución del ataque y el análisis de los resultados. De esta manera, el capítulo puso en evidencia que la evaluación de la ciberseguridad requiere un entendimiento previo del sistema y de sus condiciones de operación, destacando que la prueba de vulnerabilidad es el resultado de un proceso planificado y no una acción aislada.

4. DISPOSICIÓN FUNCIONAL Y RESULTADO DE LA PRUEBA

4.1 Introducción

El montaje de la prueba define la disposición funcional de los elementos utilizados para la ejecución de las técnicas de ciberseguridad propuestas, con el objetivo de garantizar un entorno controlado y reproducible. En esta etapa se establece cómo se conectan el medidor inteligente, la carga fantasma y los sistemas de medición, asegurando que las condiciones eléctricas permanezcan constantes durante el desarrollo de la prueba.

En el esquema de montaje considerado, el medidor vulnerable y el medidor de referencia corresponden al mismo dispositivo físico, el cual se utiliza en diferentes momentos de la prueba. Inicialmente, el medidor opera como referencia, registrando el consumo eléctrico bajo condiciones normales y sin la aplicación de estímulos. Posteriormente, el mismo medidor se somete a las técnicas de flooding y fuzzing definidas en la propuesta, pasando a desempeñar el rol de medidor bajo prueba. La utilización del mismo dispositivo como referencia y como objetivo de la prueba permite eliminar variaciones asociadas a diferencias de hardware, configuración o calibración entre medidores distintos. La comparación y discusión de los resultados se desarrollan en la etapa final del proceso metodológico, de acuerdo con la estructura definida en el diagrama general presentado en el **Anexo 5.1** y en su representación por secciones en el **Anexo 5.2**, identificada como **C-F**. En esta sección se analizan los efectos observados durante la aplicación de las técnicas de ataque, estudiando el comportamiento del medidor inteligente bajo condiciones de estrés.

4.2 Montaje de la prueba

El montaje de la prueba corresponde a la etapa experimental del proceso metodológico y se encuentra representado en el diagrama general incluido en el **Anexo 5.1**, así como en su desglose por secciones en el **Anexo 5.2**, identificado como **B2-C**. En esta fase se describe la configuración física del sistema de medición, donde un único medidor inteligente cumple simultáneamente el rol de medidor vulnerable y de referencia, operando bajo una carga fantasma que permite mantener constantes las condiciones eléctricas durante la ejecución de las pruebas de ciberseguridad.

4.2.1 Medidor vulnerables y medidor de referencia

El diagrama de conexiones eléctricas representa el esquema utilizado para interconectar el medidor inteligente *DTS27* con la red eléctrica trifásica y la carga fantasma, reproduciendo de

manera controlada las condiciones de operación reales del medidor durante la prueba de vulnerabilidad. Este esquema corresponde al montaje físico implementado en el laboratorio y define la ruta de circulación de tensiones y corrientes a través del sistema de medición.

El medidor se configura en un sistema trifásico de cuatro hilos (3P4W), en el cual las tres fases de la red eléctrica (L1, L2 y L3) y el conductor neutro (N) ingresan al medidor a través de los bornes de entrada designados. Cada fase atraviesa su respectivo canal interno de medición de corriente, permitiendo al dispositivo registrar de forma independiente el consumo asociado a cada fase. El conductor neutro se conecta directamente al borne correspondiente, estableciendo la referencia común del sistema.

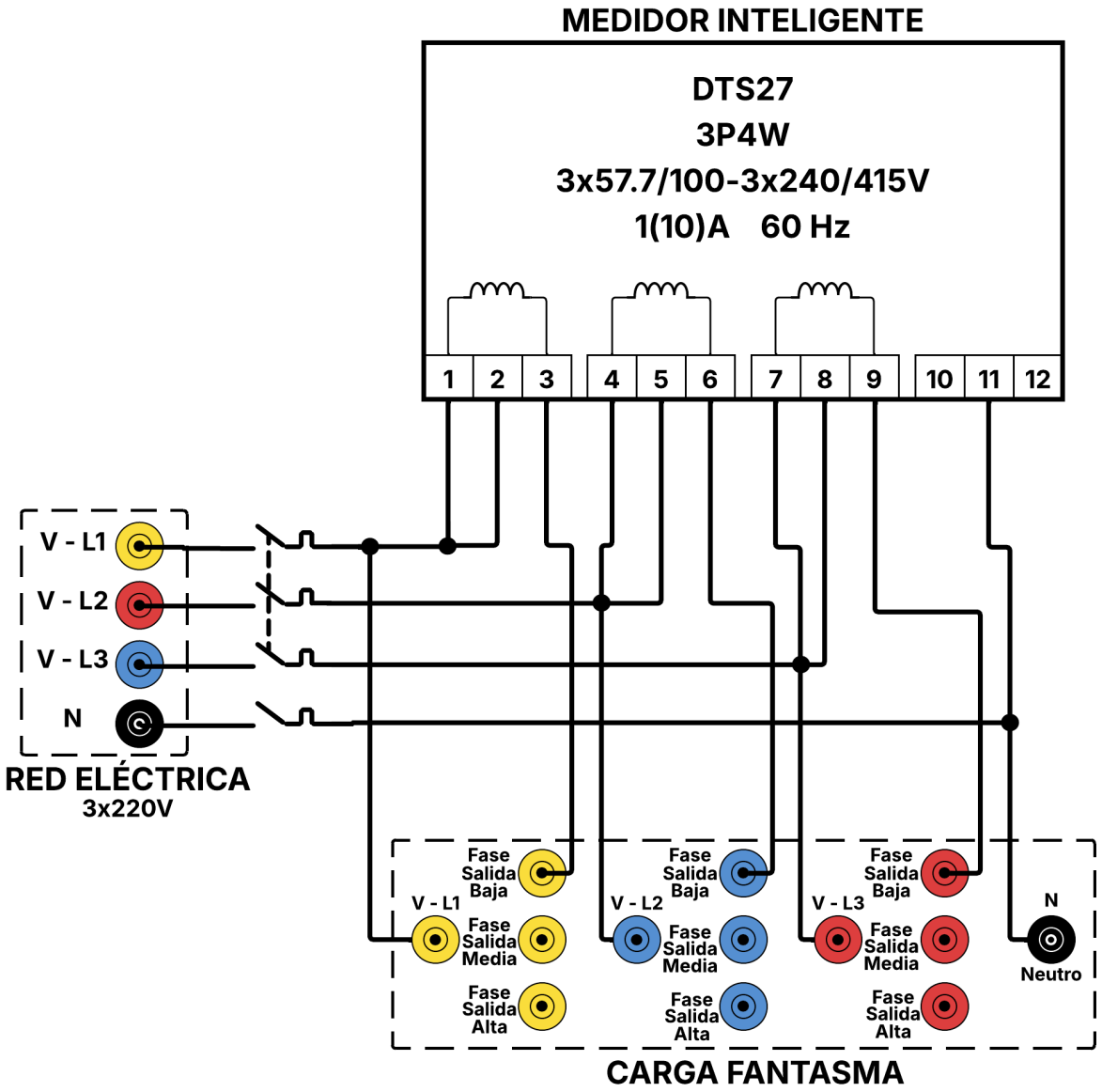
A la salida del medidor, las fases medidas se redirigen hacia la carga fantasma, manteniendo la correspondencia fase–fase entre entrada y salida. El diagrama muestra que cada fase dispone de múltiples puntos de conexión en la carga fantasma, identificados como salida baja, media y alta, los cuales permiten seleccionar distintos niveles de carga sin modificar la topología general del cableado. Esta disposición facilita la repetición de la prueba bajo diferentes condiciones de consumo manteniendo constante el esquema de conexión eléctrica.

El conductor neutro es compartido entre el medidor y la carga fantasma, cerrando el circuito eléctrico y asegurando un retorno común para las corrientes de las tres fases. De esta forma, el medidor opera en un entorno eléctricamente estable y balanceado, condición necesaria para aislar el análisis de ciberseguridad de perturbaciones propias del suministro eléctrico.

Es importante resaltar que el mismo medidor físico se utiliza tanto como medidor de referencia como medidor bajo prueba. La diferencia entre ambos roles se establece únicamente por el momento de ejecución de la prueba, sin realizar modificaciones en el esquema de conexiones eléctricas. Inicialmente, el medidor opera bajo condiciones normales de comunicación y carga; posteriormente, se aplican las técnicas de denegación de servicio mientras el montaje eléctrico permanece inalterado. Esta estrategia permite eliminar variaciones asociadas a cambios de hardware, calibración o alimentación.

En conjunto, el diagrama de conexiones define una topología eléctrica fija, reproducible y coherente con la configuración nominal del medidor inteligente, garantizando que cualquier comportamiento anómalo observado durante la prueba esté asociado al intercambio de comunicación a nivel DLMS/COSEM y no a modificaciones en las condiciones eléctricas del sistema.

Figura 4.1: Diagrama metodológico del montaje de la prueba.



Fuente: Elaboración propia.

4.2.2 Carga Fantasma Trifásica 3F

La carga fantasma trifásica 3F, fabricada por Idosde, es un dispositivo diseñado específicamente para la verificación, calibración y prueba de medidores eléctricos en entornos de laboratorio y de campo. Su función principal consiste en generar corrientes controladas en una, dos o tres fases sin requerir una carga real de potencia, permitiendo que el medidor bajo prueba registre energía como si estuviera alimentando una carga auténtica, pero con un consumo energético mínimo [99]. La operación del equipo se basa en el desacople entre el circuito de tensión y el circuito de corriente del medidor. La carga fantasma suministra al medidor una tensión de referencia (típicamente 120 V AC), mientras inyecta corrientes de prueba a través de sus circuitos de corriente. Esto

permite al medidor calcular potencia aparente y energía activa/reactiva siguiendo su lógica interna ($P = V \cdot I \cdot \cos\varphi$), aun cuando la potencia real consumida por el equipo es mínima [100].

Según el manual técnico, la carga fantasma se alimenta en un rango de 90 a 120 V AC, 50/60 Hz, utilizando la combinación Neutro + L1 como referencia de tensión. Cada fase dispone de tres niveles de corriente, etiquetados como BAJO, MEDIO y ALTO, con valores típicos de:

- Nivel BAJO: 1.5 A ± 0.5 A,
- Nivel MEDIO: 5 A ± 1 A,
- Nivel ALTO: 10 A ± 2 A.

La variación de la corriente en función de los metros de cable genera incrementos aproximados de 50 mA/m, 250 mA/m y 550 mA/m para los niveles bajo, medio y alto respectivamente, como se indica en el manual [99]. El panel frontal incorpora bornes independientes por fase:

- L1 (amarillo): entrada y salida con tres selectores de carga.
- L2 (azul): entrada y salida idéntica a L1.
- L3 (rojo): entrada y salida idéntica a L1.
- Neutro (negro): referencia común de tensión.

Cada fase es eléctricamente independiente, lo que permite configurar la carga fantasma para:

- medidores monofásicos (solo L1 + N),
- medidores bifásicos (L1 + L2 + N),
- medidores trifásicos (L1 + L2 + L3 + N),

Siguiendo los diagramas de conexión especificados en el manual [100]. El equipo incluye además un socket ANSI para conexión directa en medidores enchufables. En este modo, la carga fantasma deriva internamente la inyección de corriente a los terminales. La carga fantasma permite:

- selección de nivel de corriente para cada fase,
- operación independiente por fase,
- suspensión automática de corriente cuando se integra con el verificador AVM de Idosde,
- indicación visual mediante LED del estado operativo.

4.2.3 Consumo de energía eléctrica como variable crítica de operación y facturación

Dentro del montaje de la prueba de vulnerabilidad, el consumo de energía eléctrica se analiza a partir del **registro acumulado de energía activa importada**, identificado mediante el objeto DLMS/COSEM *OBIS 1.0.1.8.0.255*, el cual representa la energía total consumida por la carga conectada al medidor. En el ámbito de la facturación, el valor asociado al objeto OBIS 1.0.1.8.0.255 es la base fundamental para el cálculo del consumo facturable. Las empresas distribuidoras emplean este registro como insumo principal para la liquidación económica del servicio, la gestión de ingresos y el control de pérdidas técnicas y no técnicas. Cualquier alteración, inconsistencia o indisponibilidad de este dato puede derivar en errores de facturación, disputas comerciales y afectaciones en la confiabilidad del sistema de medición.

Desde la perspectiva del usuario final, este registro representa el consumo real por el cual se realiza el cobro del servicio eléctrico, siendo un elemento clave para garantizar transparencia en la facturación. La confiabilidad del valor registrado por parte de la empresa. En el contexto de la prueba de vulnerabilidad, el análisis del objeto OBIS 1.0.1.8.0.255 permite verificar si los ataques orientados a la saturación del canal de comunicación o a la generación de tráfico anómalo afectan indirectamente los procesos de medición y facturación. La comparación del valor del registro acumulado antes, durante y después de la ejecución de las pruebas posibilita evaluar la preservación de la integridad operativa del dato bajo condiciones de estrés.

4.2.4 Tipo de ataque evaluado

En el presente trabajo se optó por evaluar un ataque de denegación de servicio a nivel lógico o de protocolo, específicamente sobre la capa de aplicación del estándar DLMS/COSEM. Este tipo de ataque se caracteriza por la generación de solicitudes repetitivas que, aunque son válidas desde el punto de vista del protocolo, afectan la capacidad de la unidad de medida para procesar y responder de manera oportuna. El objetivo del ataque no es saturar la infraestructura de red, sino agotar los recursos internos del medidor, tales como la máquina de estados DLMS/COSEM, el procesador y la memoria disponible. Es importante diferenciar este enfoque de los ataques de denegación de servicio a nivel de red, los cuales buscan saturar los recursos de comunicación mediante tráfico malicioso en capas inferiores del modelo OSI, como la capa de enlace o red. Ejemplos de este tipo de ataques incluyen técnicas como SYN flood, UDP flood o ICMP flood, cuyo impacto principal se manifiesta antes de que los paquetes alcancen la capa de aplicación.

Por el contrario, el ataque de denegación de servicio lógico analizado en este estudio actúa directamente sobre la capa de aplicación, aun cuando la red se encuentra operando de manera normal. La saturación del sistema se produce como resultado del procesamiento continuo de solicitudes DLMS/COSEM, lo que genera incrementos significativos en la latencia, fallos en la asociación, timeouts y pérdida progresiva de la capacidad de respuesta del medidor frente a comandos legítimos. Desde el punto de vista funcional, este comportamiento también constituye una denegación de servicio, ya que impide o degrada de manera significativa la disponibilidad del servicio de medición. Aunque la conectividad de red no se vea interrumpida, la imposibilidad de realizar lecturas oportunas, escrituras de configuración o consultas de perfiles de carga afecta directamente la operación del sistema.

4.2.5 Introducción a la obtención y análisis de los resultados

Una vez ejecutadas las pruebas de denegación de servicio sobre la unidad de medida, se procedió a la obtención y análisis de los resultados correspondientes al comportamiento del registro acumulado de energía. Las pruebas fueron ejecutadas bajo un esquema de escalamiento

temporal controlado, compuesto por períodos de estrés de 1, 4, 8 y 12 horas, cada uno seguido por un intervalo de descanso de 30 minutos, así como una prueba adicional de 24 horas de ejecución continua. Cada prueba se mantuvo en ejecución hasta completar la totalidad de los tiempos establecidos, sin interrupciones durante los períodos de estrés definidos. Finalizada la ejecución completa de las pruebas, se tuvo en cuenta el registro horario de inicio y final de la ejecución en el que se desarrollaron las pruebas, con el fin de identificar posteriormente los valores correspondientes en el medidor. La obtención de los datos se realizó mediante la lectura del objeto OBIS 1.0.1.8.0.255, correspondiente al registro acumulado de energía, utilizando la herramienta Gurux. A partir de estas lecturas, los valores fueron recopilados de manera manual y almacenados en un software genérico de análisis de datos, en este caso Microsoft Excel, donde se construyeron las gráficas que relacionan el tiempo de ejecución (las horas en las que se desarrollaron las pruebas) con la variable analizada (registro acumulado de energía).

El proceso de generación de resultados se llevó de forma manual intencionalmente. Si bien una alternativa era en desarrollar un mecanismo automatizado que solicitara el valor del objeto OBIS al medidor en intervalos fijos y almacenará dichos datos para luego analizarlos, este enfoque no fue adoptado debido a que introduciría interferencias directas en la ejecución de la prueba y contaminación de los resultados. La solicitud periódica de datos al medidor durante la ejecución del ataque implicaría la generación de tráfico adicional legítimo, lo cual podría generar tiempos de recuperación parcial del medidor o modificar el comportamiento natural del sistema bajo condiciones de estrés. Por esta razón, se optó por un enfoque de recolección de datos posterior a la ejecución de las pruebas, garantizando que el comportamiento observado del registro acumulado de energía corresponda al impacto del ataque y no a efectos derivados del propio mecanismo de medición. Los resultados presentados a continuación corresponden a ataques de denegación de servicio a nivel lógico, implementados mediante tráfico repetitivo, con el fin de evaluar la susceptibilidad del medidor ante agotamiento de recursos.

4.2.6 Análisis del comportamiento del medidor bajo condiciones de estrés.

Con el fin de validar los resultados de la *UM* frente a ataques de DoS y determinar su grado de susceptibilidad, se realizó un análisis del comportamiento bajo un esquema de escalamiento del registro acumulado de energía en escenarios sin estrés y con estrés, aplicando pruebas de fuzzing en perfil de escritura, flooding en perfil de lectura y flooding en perfil pública.

4.2.6.1 Comportamiento del medidor en condición sin estrés

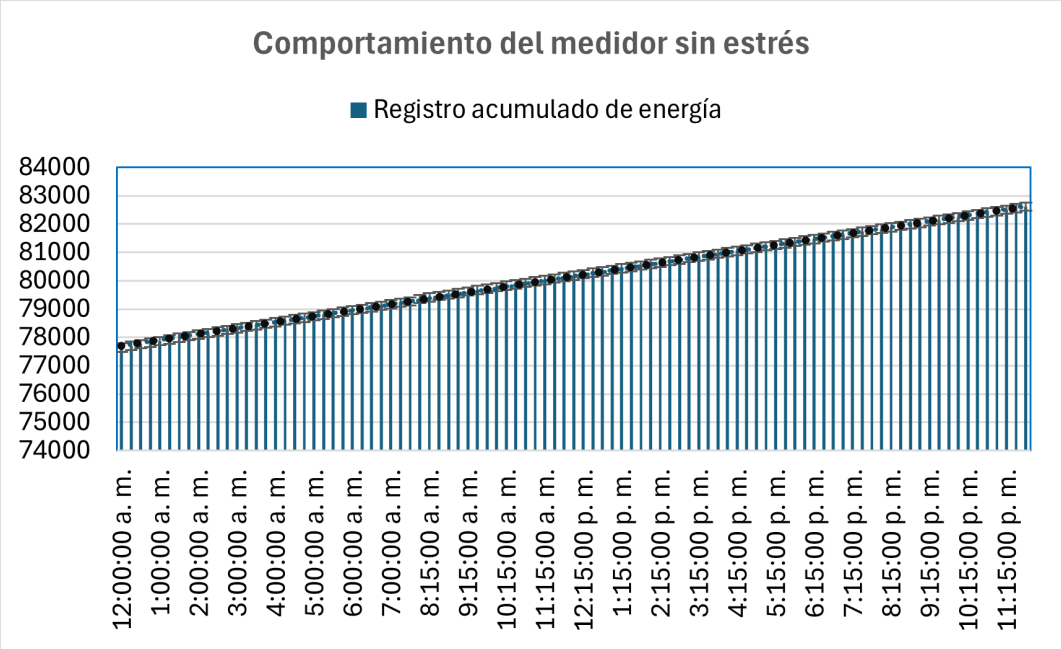
En el escenario del comportamiento del medidor sin estrés, el registro acumulado de energía presenta una tendencia creciente, continua y estable a lo largo del tiempo. La pendiente del crecimiento es prácticamente constante, lo que indica que el medidor mantiene un proceso de

medición y acumulación coherente con el consumo esperado. No se evidencian interrupciones, retrocesos ni variaciones abruptas en el valor del registro, lo cual sugiere:

- Correcta operación del proceso de medición interna.
- Estabilidad en la comunicación entre el medidor y la plataforma de adquisición (Gurux).

Este comportamiento sirve como línea base de referencia, permitiendo analizar los efectos introducidos por los escenarios de estrés **Fig 4.2**.

Figura 4.2: Comportamiento del medidor sin estrés



Fuente: Elaboración propia.

4.2.6.2 Comportamiento del medidor bajo condición de estrés

4.2.6.3 Prueba 1: Fuzzing en el perfil de escrtiura

Durante la ejecución de las pruebas con estrés, específicamente en el caso de fuzzing de escritura, se observa que el registro acumulado de energía continúa incrementándose en el tiempo, manteniendo una tendencia creciente. Sin embargo, a diferencia del escenario sin estrés, aparecen variaciones adicionales en la dinámica del registro. Estas variaciones se manifiestan principalmente en:

- Cambios leves en la pendiente del crecimiento.
- Presencia de pequeños escalamientos o irregularidades temporales, especialmente en los periodos de mayor duración de la prueba.

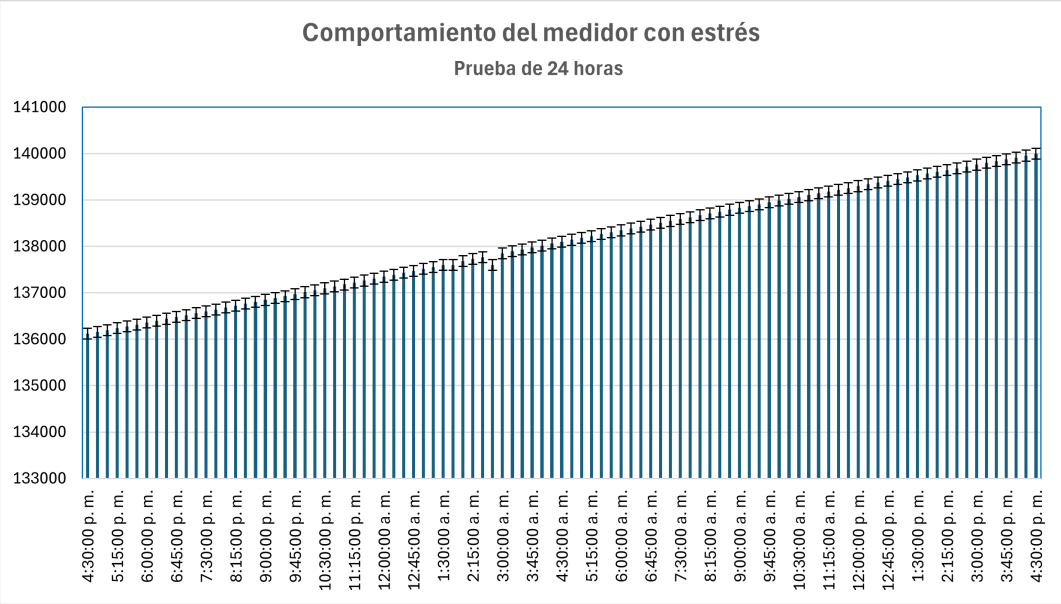
El esquema de escalamiento permite evidenciar que, a medida que aumenta el tiempo de exposición al estrés, el sistema presenta una mayor variabilidad en el registro, lo que puede asociarse a:

- Sobrecarga del canal de comunicación debido al envío repetitivo de tramas.

- Pequeñas fluctuaciones entre muestras consecutivas.

Los intervalos de descanso incorporados entre cada fase de la prueba permiten observar una recuperación parcial del comportamiento del sistema. Esto sugiere que el medidor y la infraestructura de comunicación poseen mecanismos que permiten retomar su operación normal una vez disminuye la carga de tráfico. No obstante, en las fases de mayor duración (8, 12 y 24 horas) como se observan en la **Fig 4.3** y en la **Fig 4.4**, se evidencia que la recuperación no siempre es inmediata ni idéntica al comportamiento base, lo que indica una acumulación de efectos leves residuales del estrés.

Figura 4.3: Comportamiento del medidor con estrés - Prueba fuzzing perfil escritura 24 horas.

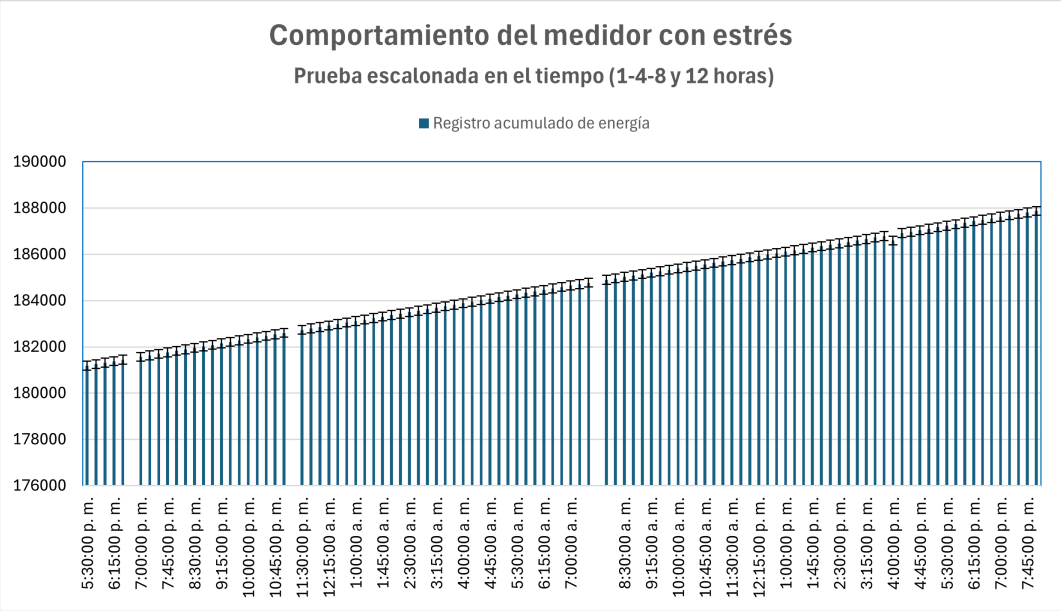


Fuente: Elaboración propia.

El hecho de que el registro de energía acumulado no se detenga ni presente pérdidas evidentes bajo condiciones de estrés indica que la función básica de medición se mantiene operativa. Sin embargo, las variaciones observadas en la estabilidad y regularidad del registro permiten identificar un grado de susceptibilidad de la unidad de medida a ataques de denegación de servicio, particularmente en términos de desempeño y calidad del servicio. Desde una perspectiva de ciberseguridad, estos resultados evidencian que: El sistema no colapsa ante el ataque, pero sí experimenta efectos medibles en su comportamiento y que la susceptibilidad no se manifiesta como una falla total, sino como una degradación progresiva con respecto al tiempo.

En este contexto, no se evidencia un comportamiento caótico asociado al tiempo, sino más bien una degradación progresiva y sostenida del desempeño, reflejada en la pérdida de uniformidad del registro. Esto sugiere que el impacto del ataque no se manifiesta necesariamente como una función directa del tiempo transcurrido, sino como una consecuencia de la persistencia del tráfico malicioso.

Figura 4.4: Comportamiento del medidor con estrés-Prueba fuzzing-escritura con escalonamiento.

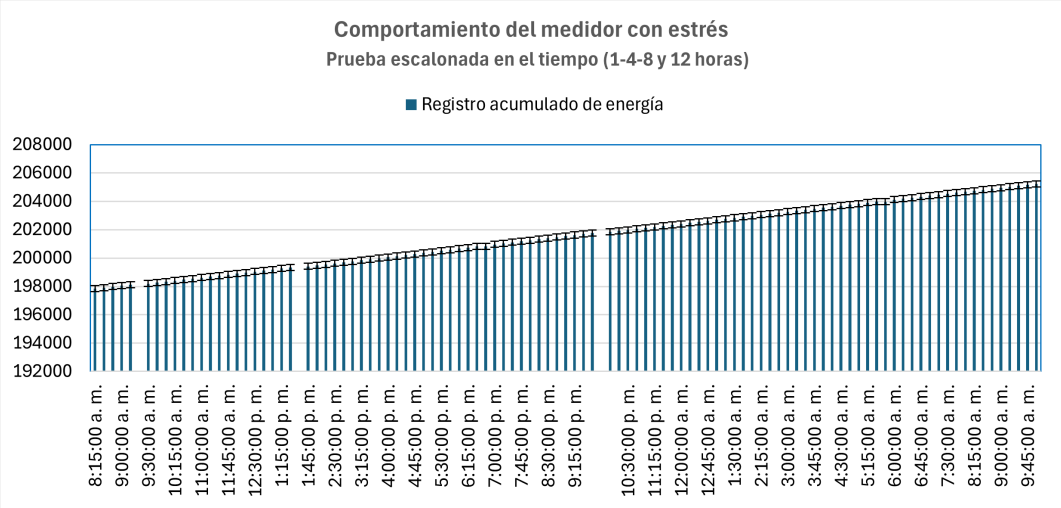


Fuente: Elaboración propia.

4.2.6.4 Prueba 2: Flooding en el perfil de lectura

En la prueba escalonada de flooding en el perfil de lecctura, el registro acumulado de energía presenta una tendencia creciente sostenida a lo largo de todas las fases de la prueba. El incremento del valor acumulado es consistente con la operación normal del medidor, lo que indica que la función de medición no se ve interrumpida por la exposición progresiva al ataque. No obstante, al analizar con mayor detalle el comportamiento del registro, se observan ligeras variaciones en la pendiente del crecimiento. Los intervalos de descanso entre cada etapa permiten evidenciar una recuperación parcial del comportamiento del sistema, reflejada en una estabilización temporal del crecimiento del registro como se observa en la **Fig 4.5**.

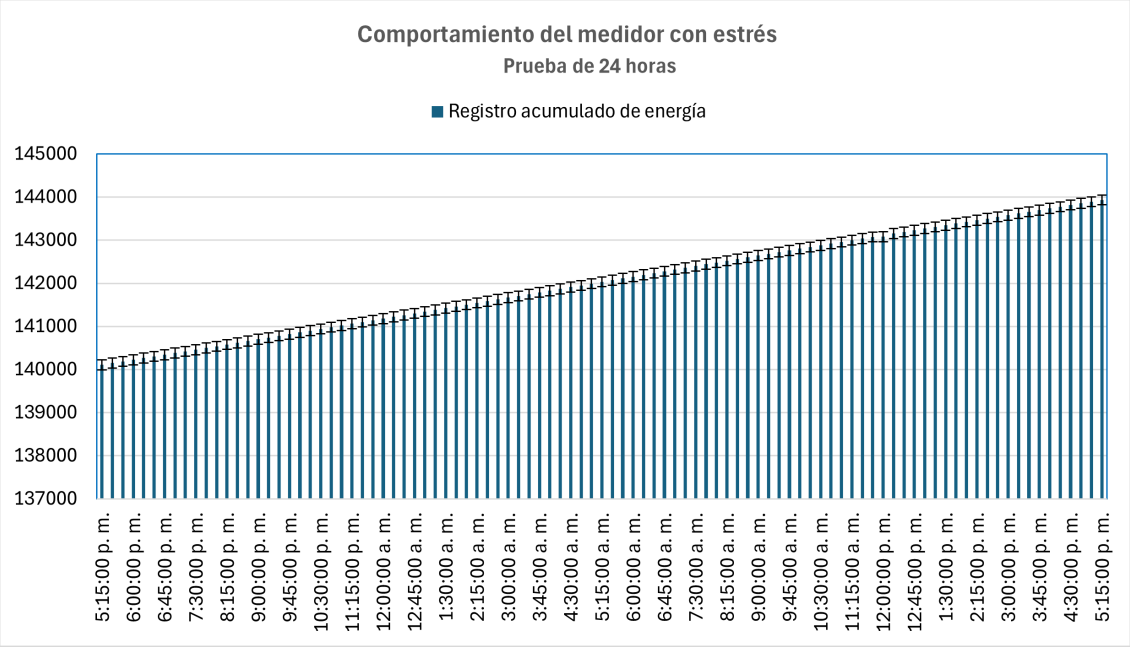
Figura 4.5: Comportamiento del medidor con estrés-Prueba flooding lectura con escalonamiento



Fuente: Elaboración propia.

En el escenario de flooding en el perfil de lectura durante 24 horas continuas, el registro acumulado de energía mantiene una tendencia ascendente uniforme, sin evidenciar interrupciones abruptas, pérdidas del valor acumulado ni comportamientos caóticos como se observan en la **Fig 4.6**. A lo largo de todo el periodo de prueba, el crecimiento del registro se presenta de manera progresiva y relativamente estable. Sin embargo, al igual que en la prueba escalonada, se identifican pequeñas fluctuaciones en la pendiente del crecimiento. Estas variaciones no comprometen la integridad de los datos medidos. Al contrastar los resultados de ambos escenarios, se puede inferir que no interfiere directamente con la función de medición del medidor.

Figura 4.6: Comportamiento del medidor con estrés - Prueba flooding perfil lectura 24 horas



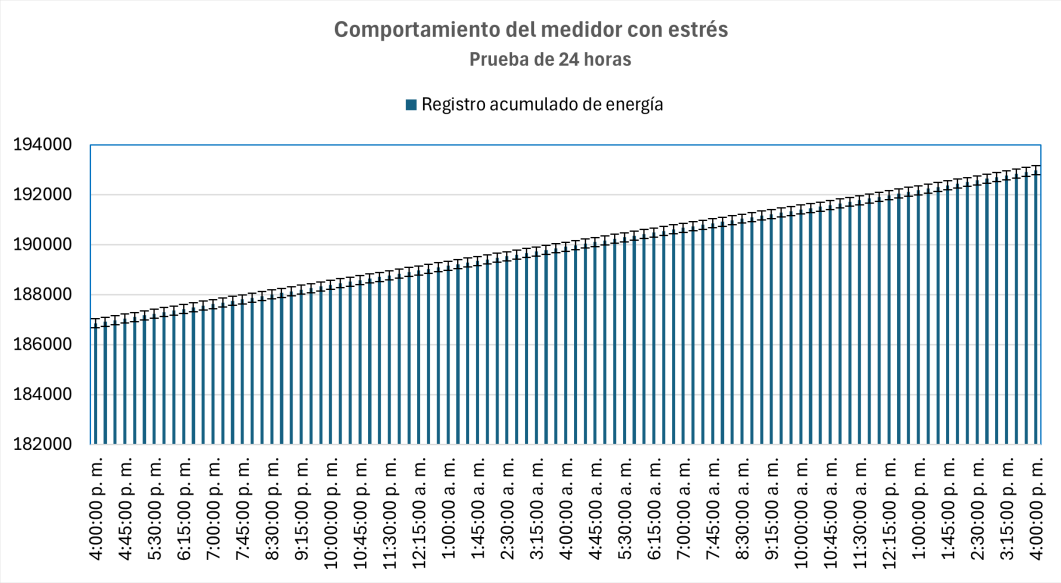
Fuente: Elaboración propia.

4.2.6.5 Prueba 3: Flooding en el perfil publico

En la prueba escalonada de flooding publico se observa una tendencia creciente y sostenida del registro acumulado de energía a lo largo de las etapas de la prueba. El incremento del valor es consistente con el comportamiento esperado de un medidor en operación continua, lo que indica que la función de medición y acumulación no se ve interrumpida por la carga adicional de solicitudes.

En la prueba de flooding en el perfil público durante 24 horas continuas, el registro acumulado de energía mantiene una tendencia ascendente uniforme, sin interrupciones abruptas ni reinicios del valor acumulado como se observan en la **Fig 4.7**. A lo largo de toda la prueba, el incremento del registro se presenta de forma más regular en comparación con la prueba escalonada, lo que sugiere una adaptación del sistema a constante solicitudes. No obstante, se evidencian leves fluctuaciones en la pendiente del crecimiento, las cuales pueden interpretarse como efectos del procesamiento continuo de un volumen de solicitudes. Estas variaciones no alteran el valor acumulado de energía.

Figura 4.7: Comportamiento del medidor con estrés - Prueba flooding perfil público 24 horas

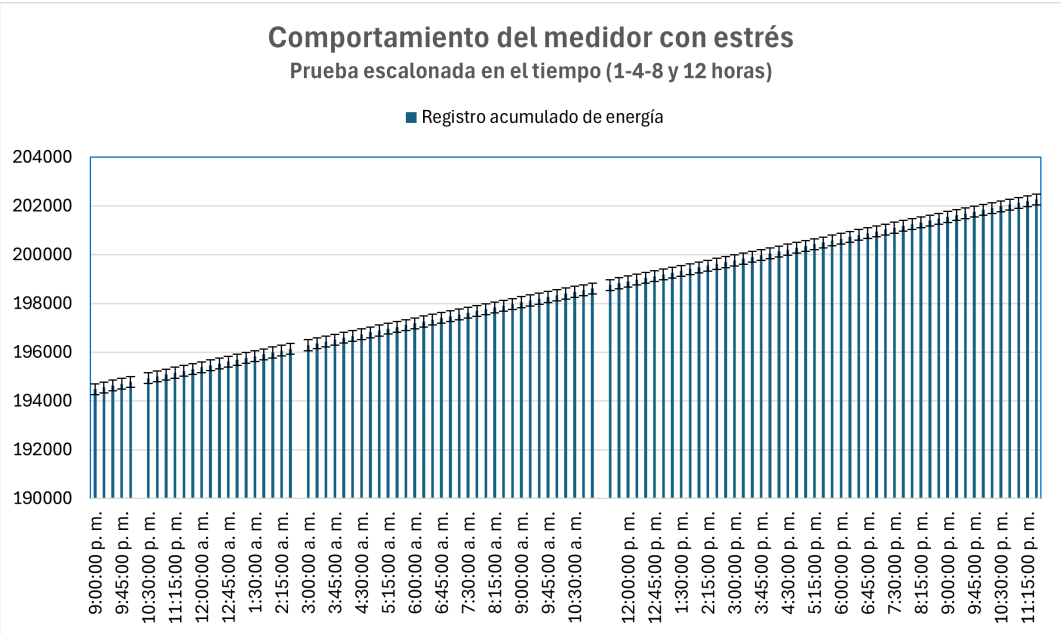


Fuente: Elaboración propia.

Estas variaciones se hacen más perceptibles en las fases de mayor duración como se observan en la **Fig 4.8**. Los intervalos de descanso entre las etapas permiten observar una recuperación parcial del comportamiento del sistema. Al comparar ambos escenarios, se puede inferir que:

- No compromete directamente la función de acumulación de energía.
- Introducir variaciones leves en la regularidad del registro, más evidentes en escenarios de estrés prolongado.

Figura 4.8: Comportamiento del medidor con estrés - Prueba flooding perfil público con escalonamiento



Fuente: Elaboración propia.

Si bien el análisis realizado se centra en la evolución temporal del registro acumulado de energía como variable principal de observación, es importante resaltar que el tiempo no constituye el único eje posible para evaluar el impacto de ataques de denegación de servicio en la unidad de medida. El enfoque adoptado permitió identificar variaciones en la estabilidad y regularidad del registro bajo condiciones de estrés prolongado; Sin embargo, el comportamiento del sistema no necesariamente se manifiesta de forma caótica o abrupta en función del tiempo. En este sentido, las pruebas de Fuzzing e Flooding pueden estar asociados a otras variables determinantes, tales como:

- Latencia en la respuesta del medidor ante solicitudes legítimas.
- Variaciones en el tiempo de procesamiento interno del medidor.
- Saturación de recursos de comunicación

Esto implica que, aunque el registro acumulado de energía mantiene una tendencia creciente, el impacto del ataque puede no reflejarse directamente como una alteración significativa en el valor medido, sino como una degradación del desempeño del sistema, observable mediante métricas complementarias. Por lo tanto, un análisis basado exclusivamente en la variable temporal puede no captar completamente el comportamiento del sistema frente a ataques de denegación de servicio. Bajo esta perspectiva, el estudio realizado constituye una aproximación válida y controlada, enfocada en el análisis del comportamiento funcional del medidor.

4.3 Evaluación de la Susceptibilidad frente a Ataques DoS

4.3.1 Definición de Métricas Cuantitativas para la Evaluación de Ataques DoS

Con el fin de cuantificar el impacto de los ataques de denegación y determinar su grado de susceptibilidad, se definieron métricas cuantitativas basadas en el desempeño de comunicaciones DLMS/COSEM del medidor inteligente. Estas métricas permiten evaluar no solo la continuidad del servicio, sino también la degradación del rendimiento del sistema bajo condiciones de estrés.

El análisis se fundamenta en un estudio de escalonamiento, en el cual se ejecutaron pruebas con duraciones de 1, 4, 8, 12 y 24 horas, separadas por intervalos de descanso. Durante cada ejecución, un script desarrollado para las pruebas registró de manera automática el número total de peticiones enviadas, las peticiones fallidas y los tiempos de respuesta de las peticiones exitosas. Los valores reportados para las métricas de disponibilidad y latencia corresponden a promedios globales de todas las ejecuciones del estudio de escalonamiento, y no a mediciones puntuales. Este enfoque permite caracterizar el comportamiento general del medidor bajo condiciones de estrés.

4.3.1.1 Tasa de Error de Disponibilidad (DER)

La Tasa de Error de Disponibilidad (DER, *DoS Error Rate*) representa el porcentaje de solicitudes enviadas al medidor que no obtuvieron una respuesta válida durante la ejecución de las pruebas. Se consideran como peticiones fallidas aquellas que resultaron en *timeout*, conexión caída, error de protocolo DLMS/COSEM, rechazo o fallo en la asociación.

$$DER = \left(\frac{\text{Peticiones Fallidas}}{\text{Total de Peticiones Enviadas}} \right) \times 100 \tag{4.1}$$

Esta métrica cuantifica el nivel de indisponibilidad del dispositivo bajo ataque. Un valor de DER cercano a 0 % indica un sistema completamente disponible, mientras que valores elevados evidencian una degradación del servicio de gestión remota, característica de escenarios de denegación de servicio. Al tratarse de un valor promedio global, el DER refleja el impacto acumulado del ataque a lo largo de todas las ejecuciones del estudio de escalonamiento.

4.3.1.2 Índice de Latencia Acumulada (ALI / RTT)

El Índice de Latencia Acumulada (ALI) corresponde al tiempo promedio de ida y vuelta (*Round Trip Time*) de las peticiones que fueron respondidas exitosamente durante los escenarios de estrés.

$$ALI = \frac{\sum \text{Tiempo de respuesta de peticiones exitosas}}{\text{Total de peticiones exitosas}} \tag{4.2}$$

Esta métrica permite evaluar la degradación del rendimiento del sistema bajo ataque. Incluso cuando el medidor continúa respondiendo, un incremento significativo del ALI respecto a la línea base indica saturación de recursos internos y pérdida de eficiencia operativa. Al ser un valor promedio global, el ALI representa el comportamiento general del medidor durante todo el estudio de escalonamiento y no una condición transitoria.

4.3.2 Análisis de la susceptibilidad de las pruebas de DoS

El análisis conjunto de los tres escenarios de ataque evidencia que la susceptibilidad de la unidad de medida no se manifiesta de una única forma, sino a través de distintos patrones de degradación que dependen del tipo de tráfico malicioso generado.

Desde el punto de vista de la *disponibilidad*, el ataque de *Flooding Público* presenta una

susceptibilidad moderada, reflejada en una disminución parcial de la capacidad de respuesta del medidor. Aunque el sistema no colapsa completamente, la presencia de peticiones fallidas reduce la confiabilidad de la gestión remota, evidenciando que el dispositivo es vulnerable ante ataques de bajo nivel de complejidad.

En el caso del *Flooding de Lectura*, la disponibilidad nominal se mantiene en el 100 %, lo que podría interpretarse inicialmente como un comportamiento resiliente. No obstante, esta métrica por sí sola resulta insuficiente para caracterizar la susceptibilidad del sistema, ya que el medidor continúa aceptando solicitudes a costa de un consumo intensivo de recursos internos.

Al analizar la *latencia*, se observa que el *Flooding Público* genera un incremento moderado del tiempo de respuesta, mientras que el *Flooding de Lectura* produce una degradación severa del rendimiento, con tiempos de respuesta elevados con respecto a la linea base. Este comportamiento imposibilita la operación efectiva del sistema y corresponde a un escenario de denegación de servicio por agotamiento de recursos.

Por su parte, el *Fuzzing de Escritura* presenta una alta susceptibilidad tanto en términos de disponibilidad como de latencia. La elevada tasa de fallos en las solicitudes de escritura, combinada con el incremento del tiempo de respuesta, compromete de manera crítica las funciones de configuración, control y mantenimiento remoto del medidor, consolidándose como el escenario de mayor impacto entre las pruebas.

En conjunto, los resultados confirman que la susceptibilidad de la unidad de medida frente a ataques de denegación de servicio debe evaluarse considerando simultáneamente métricas de disponibilidad y latencia. Un ataque puede no generar una interrupción inmediata del servicio, pero sí provocar una degradación progresiva del rendimiento y la eficiencia operativa.

Tabla 4.1: Comparativa de resultados de las pruebas de DoS en la unidad de medida

Tipo de prueba	**DER**	**Disponibilidad**	**ALI promedio**	**Análisis de impacto**
Flooding Público	16.67 (%)	83.33 (%)	0.1884 (s)	Degradación moderada del canal de comunicaciones. Se presentan fallos intermitentes en la gestión remota; sin embargo mantiene su operación.
Flooding de Lectura	0.00 (%)	100.00 (%)	90.83 (s)	Alta degradación del rendimiento sin pérdida de disponibilidad nominal. El elevado tiempo de respuesta evidencia un escenario de agotamiento de recursos que afecta la viabilidad del sistema.
Fuzzing de Escritura	87.70 (%)	12.30 (%)	0.4620 (s)	Escenario crítico de denegación de servicio. La alta tasa de fallos y el incremento de la latencia comprometen las funciones de gestión del medidor.

Nota: Los valores presentados en esta tabla corresponden a los promedios obtenidos a partir del estudio de escalonamiento temporal (1, 4, 8, 12 y 24 horas), calculados de manera automática por los scripts de prueba. Estos resultados no representan un único intervalo de ejecución, sino el comportamiento global del medidor bajo condiciones de estrés sostenido.

4.4 Discusión

Durante este capítulo se discutieron los resultados obtenidos a partir de la prueba de vulnerabilidad realizada sobre la unidad de medida en un entorno AMI, permitiendo evidenciar el impacto que un ataque de denegación de servicio puede generar sobre la disponibilidad del sistema. A través del análisis del comportamiento del dispositivo bajo condiciones de estrés, se logró identificar cómo este tipo de amenazas puede afectar la operación normal del proceso de medición, resaltando la relevancia de la unidad de medida como un componente crítico. Los resultados obtenidos muestran que la susceptibilidad del medidor no se manifiesta de forma uniforme, sino que depende del tipo de ataque y de la naturaleza de las operaciones DLMS/COSEM involucradas. Mientras que el flooding sobre objetos de acceso público genera una degradación moderada de las comunicaciones, el flooding de lectura con sesión válida evidencia un escenario de denegación de servicio por agotamiento de recursos, caracterizado por tiempos de respuesta excesivos aun cuando la disponibilidad nominal se mantiene. Por su parte, el fuzzing de escritura representa el escenario más crítico, al combinar una alta tasa de indisponibilidad con un incremento significativo de la latencia.

Es importante resaltar que los efectos observados no corresponden a una saturación de red, sino a una degradación inducida en la capacidad de procesamiento del medidor. Este comportamiento confirma que la denegación de servicio puede manifestarse incluso cuando la conectividad de red permanece operativa, afectando directamente la disponibilidad funcional de la unidad de medida.

Así mismo, el alcance del estudio permitió identificar que, si bien la prueba se realizó sobre un único componente y un tipo específico de ataque, los escenarios evaluados representan situaciones posibles en implementaciones reales de sistemas AMI. Esto resalta la necesidad de fortalecer las evaluaciones de ciberseguridad considerando otros componentes de la infraestructura, diferentes tecnologías de comunicación y nuevos vectores de ataque, de manera que se logre una visión más completa de los riesgos a los que están expuestos los sistemas de medición avanzada.

Finalmente, los resultados discutidos en este capítulo evidencian que la ciberseguridad en AMI debe ser concebida como un proceso continuo, en el cual las pruebas de vulnerabilidad constituyen una herramienta fundamental para identificar debilidades y apoyar la toma de decisiones técnicas. En este contexto, el trabajo aporta a la discusión académica y técnica sobre la necesidad de impulsar prácticas de evaluación sistemática de ciberseguridad en la unidad de medida.

5. CONCLUSIONES Y TRABAJOS FUTUROS

5.1 Conclusiones Generales

A partir del desarrollo de este trabajo se evidenció que la evaluación de la ciberseguridad en sistemas AMI, y particularmente en la unidad de medida, requiere un enfoque integral que articule aspectos técnicos, normativos y operativos. El diagrama metodológico propuesto permitió estructurar de manera ordenada el proceso para la realización de una prueba de vulnerabilidad, integrando desde la revisión de estándares y normativas, hasta la implementación y analisis en un entorno de laboratorio controlado. De esta forma, se establece que la finalidad de la prueba no es únicamente la ejecución de un ataque de denegación de servicio, sino la comprensión del sistema AMI como un todo y de las condiciones necesarias para evaluar su resiliencia de manera adecuada.

Así mismo, se identificó que la unidad de medida constituye un punto crítico dentro de la arquitectura AMI, debido a su rol fundamental en la adquisición de datos y la facturación. La incorporación de protocolos de comunicación estandarizados como DLMS/COSEM, junto con la creciente digitalización y conectividad de los medidores inteligentes, incrementa de manera significativa la superficie de ataque. Esto genera un interés por parte de actores maliciosos en explotar vulnerabilidades que afectan principalmente la disponibilidad del servicio. El estudio evidencia que los ataques de denegación de la unidad de medida no se restringen a la saturación de la infraestructura de red, sino que pueden materializarse a nivel lógico mediante el uso intensivo del protocolo DLMS/COSEM. Este tipo de ataques afecta directamente la capacidad del medidor para procesar solicitudes, comprometiendo la disponibilidad y el rendimiento del servicio de medición, aun cuando las condiciones de conectividad de red se mantienen operativas.

El diagrama desarrollado actúa como una guía que conduce de manera progresiva hacia la ejecución de la prueba de vulnerabilidad, dejando en evidencia que la ciberseguridad en sistemas AMI no se limita a la aplicación de una técnica de ataque específica. Por el contrario, el esquema resalta la existencia de un proceso previo indispensable que incluye el entendimiento del sistema, la identificación de riesgos, la definición de criterios técnicos y la preparación del entorno de prueba. Este enfoque permite adoptar las técnicas de ciberseguridad de forma consciente y estructurada, asegurando que la prueba de vulnerabilidad sea el resultado de un proceso metodológico y no una acción aislada dentro de la evaluación de la unidad de medida.

Por otro lado, el uso de estándares y tecnologías ampliamente adoptadas, aunque facilita la interoperabilidad y la integración de los sistemas AMI, también implica que las vulnerabilidades y técnicas de ataque puedan ser replicadas en distintos contextos. En este escenario, el enfoque metodológico propuesto se presenta como una herramienta que permite evaluar de manera

estructurada la exposición de la unidad de medida ante ataques DoS, así como sentar las bases para futuras pruebas orientadas a otros vectores de ataque. La aplicación de estándares de ciberseguridad y buenas prácticas contribuye a mejorar la capacidad de respuesta y el fortalecimiento de los mecanismos de protección.

Finalmente, este trabajo pone de manifiesto la necesidad de fortalecer la ciberseguridad en los sistemas AMI como un componente estratégico para la confiabilidad y sostenibilidad del sector eléctrico. Los resultados obtenidos evidencian la importancia de promover evaluaciones de seguridad en la unidad de medida, así como de fomentar una mayor apropiación de las prácticas de ciberseguridad en entornos académicos y de investigación. Se hace necesario impulsar el desarrollo de capacidades técnicas y la continuidad de investigaciones que permitan anticipar riesgos, mejorar la resiliencia de los sistemas de medición avanzada y acompañar de manera segura el proceso de modernización de las redes eléctricas inteligentes.

5.2 Trabajos Futuros

A partir de los resultados obtenidos y del alcance definido en este trabajo de grado, se identifican diversas líneas de investigación que se pueden desarrollar para profundizar el análisis de la ciberseguridad en sistemas AMI y estarían enfocados en:

- Implementar una prueba de ciberseguridad en la unidad de medida incorporando tecnologías de comunicación de las capas bajas, tales como PLC, RF Mesh o redes celulares, con el fin de analizar escenarios de telemedición y su impacto sobre la disponibilidad del sistema AMI.
- Analizar otros tipos de ciberataques distintos a la denegación de servicio, como la manipulación de datos de medición, ataques de suplantación de identidad, ataques de repetición y accesos no autorizados, permitiendo evaluar la integridad y disponibilidad.
- Implementar mecanismos de mitigación y detección de ataques, tales como sistemas de monitoreo de tráfico, técnicas de detección de anomalías o políticas de control de acceso más robustas, orientadas a fortalecer la resiliencia de los sistemas AMI.
- Implementar un esquema experimental que incorpore un segundo dispositivo de medición operando de manera simultánea bajo las mismas condiciones, junto con la automatización del proceso de recolección de datos, con el fin de establecer un control comparativo y capturar métricas complementarias, como la latencia en tiempo real y otros indicadores de desempeño que permitan un análisis más detallado del impacto de los ataques sobre los sistemas AMI.
- Estudiar la aplicación de pruebas de ciberseguridad en entornos avanzados de simulación y gemelos digitales, como laboratorios tipo *LiveLabs*, que permitan reproducir escenarios de ataque y defensa sin afectar infraestructuras reales.

REFERENCIAS

[1] National Institute of Standards and Technology (NIST), "NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0." https://www.nist.gov/publications/nist-framework-and-roadmap-smart-grid-interoperability-standards-release-30. [Online; acceso 1-Octubre-2024].

[2] IEEE, "Smart Grid: Cyber Security Challenges and Solutions." https://ieeexplore.ieee.org/document/4596535, 2008. [Online; acceso 17-Septiembre-2024].

[3] IEEE, "Cybersecurity of Smart Grids." https://ieeexplore.ieee.org/document/7991195, 2017. [Online; acceso 13-Septiembre-2024].

[4] IEEE, "Smart Meter Security." https://ieeexplore.ieee.org/document/5736035, 2010. [Online; acceso 13-Septiembre-2024].

[5] Dragos Inc., "CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations," tech. rep., Dragos, 2017.

[6] Smart Grids Info, "Comunicación del reto de ciberseguridad en infraestructuras de medición avanzada." https://www.smartgridsinfo.es/comunicaciones/comunicacion-reto-ciberseguridad-infraestructuras-medicion-avanzada. [Online; acceso 10-Marzo-2025].

[7] National Institute of Standards and Technology (NIST), "Framework for Improving Critical Infrastructure Cybersecurity." https://www.nist.gov/cyberframework, 2018. [Online; acceso 1-Octubre-2024].

[8] Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC), "NTC 6079:2021. Requisitos para sistemas de infraestructura de medición avanzada (AMI) en redes de distribución de energía eléctrica." https://tienda.icontec.org/gp-ntc-6079-2021.html, 2021. [Online; acceso 1-Octubre-2024].

[9] H. K. O. A. Alvarez and S. Kumar, "Experimental evaluation of smart electric meters' resilience under cyber security attacks," *IEEE Access*, vol. 11, pp. 55349–55360, 2023. [Online; acceso 1-Octubre-2024].

[10] E. G.-L. A. Salazar-Bermúdez, W. Alfonso-Morales, and D. Zuluaga, "Desafíos en la ciberseguridad con la implementación de las smart grids," Mar. 2023. [Online; acceso 2-Octubre-2024].

[11] E. R. G. for Electricity and G. (ERGEG), "Conclusions paper on smart grids (ref. e10-eqs-38-05), corrigendum," tech. rep., Council of European Energy Regulators (CEER), June 2010.

[12] N. I. of Standards and Technology, "Framework and roadmap for smart grid interoperability standards." Recuperado de: `https://www.nist.gov/`, 2010. [Online; acceso 1-Octubre-2024].

[13] E. P. R. I. (EPRI), "Estimating the costs and benefits of the smart grid," tech. rep., Electric Power Research Institute, Palo Alto, CA, USA, 2011.

[14] EPRI, "Common information model primer: Eighth edition." in 3002024188., 238, EPRI, 2022.

[15] I. E. C. (IEC), "Iec 61970: Energy management system application program interface (ems-api)." IEC, 2020.

[16] I. E. C. (IEC), "Iec 61968: Application integration at electric utilities - system interfaces for distribution management." IEC, 2020.

[17] I. E. C. (IEC), "Iec 62325: Framework for energy market communications." IEC, 2018.

[18] N. I. of Standards and T. (NIST), "Nist framework and roadmap for smart grid interoperability standards, release 4.0," 2021. Accessed: Dec. 15, 2021.

[19] S. G. Grijalva and M. A. Tariq, "Prosumer-based smart grid architecture enables a flat, sustainable electricity industry," in *Proc. IEEE PES Innovative Smart Grid Technologies (ISGT)*, pp. 1–6, 2011.

[20] N. I. of Standards and T. (NIST), "Nist cloud computing standards roadmap, special publication 1108r4," tech. rep., U.S. Department of Commerce, June 2024.

[21] J. Boal, "Smart grid." Recuperado de: `http://www.dea.icai.upco.es/sadot/Comunicaciones/avanzadas/Smart%20grid%20-%20Jaime%20Boal.pdf`, 2010. [Online; acceso 1-Octubre-2024].

[22] G. A. C. (), "Gridwise interoperability framework." Available at: `https://www.gridwiseac.org/`, 2015.

[23] K. C. Budka, J. G. Deshpande, and M. Thottan, *Communication Networks for Smart Grids: Making Smart Grid Real*. Springer Science & Business Media, 2014.

[24] I. E. C. (IEC), "Power systems management and associated information exchange – Part 1: Common information model (CIM) base," 2018.

[25] Grand View Research, "Industrial Internet of Things Market Size, Share & Trends Analysis Report." https://www.grandviewresearch.com/industry-analysis/industrial-internet-of-things-iiot-market. [Online; acceso 1-Octubre-2024].

[26] CEN-CENELEC-ETSI Smart Grid Coordination Group, "SG-CG/M490/H Smart Grid Information Security," tech. rep., CEN-CENELEC-ETSI Smart Grid, 2014.

[27] "Power systems management and associated information exchange - Data and communications security - Part 5: Security for 60870-5 and derivatives," 2013.

[28] "Information technology — Security techniques — Information security management systems — Overview and vocabulary," Feb. 2018.

[29] International Society of Automation, "ISA/IEC 62443 Series of Standards." [Online; 12. Ene. 2023].

[30] National Institute of Standards and Technology (NIST), "Guidelines for smart grid cybersecurity," sep 2014.

[31] S. Untiveros, "Explorando el Estándar IEEE 1686-2019: Ciberseguridad en Tecnologías Operativas (OT)," Dec. 2023.

[32] Consejo Nacional de Operación (CNO), "Acuerdo 1502: Por el cual se aprueba la actualización de la guía de ciberseguridad y se modifican algunos plazos." [En línea]. Disponible en: `https://www.cno.org.co/content/acuerdo-1502-por-el-cual-se-aprueba-la-actualizacion-de-la-guia-de-ciberseguridad-y-se`, Dec. 2021.

[33] J. C. Guerrero and A. O. Aguirre, "Acuerdo 1502," Dec. 2021.

[34] Consejo Nacional de Operación (CNO), "Acuerdo 1960: Por el cual se aprueba la actualización de la guía de ciberseguridad y se modifican algunos plazos." [En línea]. Disponible en: `https://www.cno.org.co/content/acuerdo-1960-por-el-cual-se-aprueba-la-actualizacion-de-la-guia-de-ciberseguridad-y-se`, Apr. 2025.

[35] S. Y. G. Benítez, "SEGURIDAD DIGITAL Y GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN," Feb. 2023.

[36] Presidencia de la República de Colombia, "Decreto 338 de 2022," 2022. Último acceso: 13 de marzo de 2025.

[37] "Documento Conpes 3701," July 2011.

[38] C. Clark, H. Strohmier Berry, B. Sullivan, N. Maroney, and J. Galbraith, "Malware exploitation and vulnerability assessment of cve-2024-38063 in windows 10 and 11 in academic networks cybersecurity," 2025. Proceedings of the 13th International Symposium on Digital Forensics and Security (ISDFS), DOI: 10.1109/ISDFS65363.2025.11011991.

[39] M. A. A. Nikoleta, P. Iouila and B. Marcello, "Smart grid laboratories inventory 2022," tech. rep., Publications Office of the European Union, Luxembourg, 2022. online.

[40] DNV, "Dlms test facilities," Mar. 2023. Accessed: Mar. 20, 2025.

[41] Tecnalia, "Ensayos de concentradores de datos," Mar. 2025. Accessed: Mar. 20, 2025.

[42] CESI, "Smart metering laboratories - cesi," Mar. 2025. Accessed: Mar. 20, 2025.

[43] Trialog, "Trainings – g3-plc and dlms/cosem," Mar. 2025. Accessed: Mar. 20, 2025.

[44] Instituto Tecnológico de la Energía (ITE), "Certificación comunicaciones prime - ite," Aug. 2025. Accessed: Aug. 10, 2025.

[45] Silicon Labs, "Smart metering wireless solutions - silicon labs," Aug. 2025. Accessed: Aug. 10, 2025.

[46] Smart Metering Systems (SMS), "Smart metering test lab | sms," Aug. 2025. Accessed: Aug. 10, 2025.

[47] SINTEF, "Smart grid laboratory," Aug. 2025. Accessed: Aug. 10, 2025.

[48] CCLab, "Cclab solution: Smart metering solutions," Aug. 2025. Accessed: Aug. 10, 2025.

[49] Applus+ Laboratories, "Smart meter security evaluations," Aug. 2025. Accessed: Aug. 10, 2025.

[50] Central Power Research Institute (CPRI), "Metering protocol laboratory – metering and utility automation division," Aug. 2025. Accessed: Aug. 10, 2025.

[51] EDP Labelec, "Qualification and inspections | edp.com," Aug. 2025. Accessed: Aug. 10, 2025.

[52] UFD – Grupo Naturgy, "Laboratory - distribuidora de electricidad del grupo naturgy," Aug. 2025. Accessed: Aug. 10, 2025.

[53] Kalkitech, "Smart metering consultancy service | smart meter rollout," Aug. 2025. Accessed: Aug. 10, 2025.

[54] TÜV Rheinland, "Smart grid product testing | wo | tÜv rheinland," Aug. 2025. Accessed: Aug. 10, 2025.

[55] C.-C. Sun, D. J. S. Cardenas, A. Hahn, and C.-C. Liu, "Intrusion detection for cybersecurity of smart meters," *IEEE Transactions on Smart Grid*, vol. 12, pp. 612–622, Jan. 2021.

[56] A. Hahn, A. Ashok, S. Sridhar, and M. Govindarasu, "Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid," *IEEE Transactions on Smart Grid*, vol. 4, pp. 847–855, Jun. 2013.

[57] T. Bhatt, C. Kotwal, and N. Chaubey, "Implementing and examination of eigrp ospf rip routing protocol in ami network for ddos attack using opnet," *International Journal of Recent Technology and Engineering (IJRTE)*, vol. 8, pp. 3776–3783, Sep. 2019.

[58] D. J. S. Raja, N. Hemavathi, R. Sriranjani, and P. Arulmozhi, "Integrated game theoretic and honeypot based distributed denial of service attack detection and mitigation in advanced metering infrastructure," *IEEE Transactions on Instrumentation and Measurement*, vol. 74, pp. 1–12, 2025.

[59] S. Garg, K. Kaur, G. Kaddoum, J. J. P. C. Rodrigues, and M. Guizani, "Secure and lightweight authentication scheme for smart metering infrastructure in smart grid," *IEEE Transactions on Industrial Informatics*, vol. 16, pp. 3548–3556, May 2020.

[60] B. Bhushan, G. Chaudhary, K. Sharma, and A. Kumar, "Security challenges in smart grid implementation: An overview," in *Intelligent Data Communication Technologies and Internet of Things (ICICI 2020)*, vol. 59 of *Lecture Notes on Data Engineering and Communications Technologies*, pp. 629–641, Springer, Singapore, 2020.

[61] K. I. Sgouras, A. N. Kyriakidis, and D. P. Labridis, "Short-term risk assessment of botnet attacks on advanced metering infrastructure," *IET Cyber-Physical Systems: Theory & Applications*, 2023. Early Access.

[62] Y. Wu, T. Zhu, Q. Zhang, Y. Yi, and J. Li, "Impact of distributed denial-of-service attack on advanced metering infrastructure," in *Proc. IEEE International Conference on Communications (ICC)*, pp. 1029–1034, IEEE, 2014.

[63] P. Yi, T. Zhu, Q. Zhang, Y. Wu, and L. Pan, "Puppet attack: A denial of service attack in advanced metering infrastructure network," *Journal of Network and Computer Applications*, vol. 51, pp. 88–96, 2015.

[64] P. D. Halle and S. S., "Secure routing through refining reliability for wsn against dos attacks using aodsd2v2 algorithm for ami," *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, vol. 8, pp. 282–289, Aug. 2019.

[65] S. Tufail, I. Parvez, S. Batool, and A. Sarwat, "A survey on cybersecurity challenges, detection, and mitigation techniques for the smart grid," *Energies*, vol. 14, p. 5894, Sep. 2021.

[66] Z. Baig, S. Zeadally, A. Ibrahim, and E. S. Al-Shaer, "Future challenges for smart grids: Cybersecurity and privacy," *IEEE Computer*, vol. 50, pp. 50–59, May 2017.

[67] M. Ozay, I. H. Cavdar, I. Erguler, A. Zengin, A. Levi, and E. C. Karasan, "Machine learning methods for attack detection in the smart grid," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 27, pp. 1773–1786, Aug. 2016.

[68] S.-Y. Tan, C. Yuen, W.-C. Wong, R. Lin, and B. S. Lee, "Impact of cybersecurity attacks on smart grids," *IEEE Transactions on Smart Grid*, vol. 9, pp. 5171–5180, Sep. 2017.

[69] M. Z. Gunduz and R. Das, "Cyber-security on smart grid: Threats and potential solutions," *Computer Networks*, vol. 169, p. 107094, Mar. 2020.

[70] M. Z. Gunduz and R. Das, "Analysis of cyber-attacks on smart grid applications," in *Proc. IEEE International Conference on Computer Science and Engineering (UBMK)*, IEEE, 2018.

[71] L. Wei, L. P. Rondon, A. Moghadasi, and A. I. Sarwat, "Review of cyber-physical attacks and counter defense mechanisms for advanced metering infrastructure in smart grid," in *Proc. IEEE International Conference on Smart Grid Communications (SmartGridComm)*, IEEE, 2018.

[72] T. Jamal, Z. Haider, S. A. Butt, and A. Chohan, "Denial of service attack in cooperative networks," in *Proc. 12th International Conference on Digital Society (ICDS)*, (Rome, Italy), IARIA, 2018.

[73] J. Mirkovic and P. Reiher, "A taxonomy of ddos attack and ddos defense mechanisms," *ACM SIGCOMM Computer Communication Review*, vol. 34, pp. 39–53, Apr. 2004.

[74] Y. Guo, C.-W. Ten, S. Hu, and W. W. Weaver, "Modeling distributed denial of service attack in advanced metering infrastructure," in *Proc. IEEE Power and Energy Society General Meeting (PESGM)*, (Denver, CO, USA), pp. 1–5, IEEE, 2015.

[75] D. Grochocki, J. H. Huh, R. Berthier, R. Bobba, W. H. Sanders, A. A. Cárdenas, and J. G. Jetcheva, "Ami threats, intrusion detection requirements and deployment recommendations," in *Proc. IEEE Third International Conference on Smart Grid Communications (SmartGridComm)*, (Tainan City, Taiwan), pp. 395–400, IEEE, 2012.

[76] T. Mahjabin, Y. Xiao, G. Sun, and W. Jiang, "A survey of distributed denial-of-service attack prevention and mitigation techniques," *Journal of Network and Computer Applications*, vol. 67, pp. 147–165, 2017.

[77] G. Hernandez, M. Colak, and S. Yilmaz, "The role of smart meters in smart grid development," *IEEE Access*, vol. 8, pp. 147899–147913, Aug. 2020.

[78] A. Bose, "Smart transmission grid applications and their supporting infrastructure," *Proceedings of the IEEE*, vol. 99, pp. 928–936, Jun. 2011.

[79] H. Gharavi and R. Ghafurian, "Smart grid: The electric energy system of the future," *Proceedings of the IEEE*, vol. 99, pp. 917–921, Jun. 2011.

[80] C. Rottondi, S. Fontana, and G. Verticale, "Analysis of privacy in smart metering systems: Requirements and threats," *Computer Networks*, vol. 57, pp. 1344–1359, May. 2013.

[81] Comisión de Regulación de Energía y Gas (CREG), "Resolución 40072 de 2018: Reglamento de medición inteligente de energía eléctrica (miee)." [En línea]. Disponible en: `https://www.creg.gov.co/sites/default/files/normativa/creg40072_2018.pdf`, May. 2018.

[82] N. Saputra and K. Kadir, "Smart meter design for smart grid applications," 2021.

[83] M. Popa, "Smart metering system architecture: Components and communication technologies," 2019.

[84] International Electrotechnical Commission, "Electricity metering—data exchange for metering reading, tariff and load control—part 61: Object identification system (obis)," 2022.

[85] Laboratorio AMI – Universidad del Valle, "Formación ami: Evaluación de tecnologías smart grid e infraestructura de medición avanzada (ami)." Presentación técnica, Jun. 2024. En colaboración con Metrum Colombia.

[86] INCIBE-CERT, "Guía de seguridad en protocolos industriales smart grid," tech. rep., Instituto Nacional de Ciberseguridad de España (INCIBE), 2017. Secciones 4.3–4.5: Seguridad en protocolos PLC (PRIME y G3-PLC).

[87] G3-PLC Alliance, "G3-plc alliance specification v1.2," 2017. Physical and MAC layer specification with security extensions.

[88] PRIME Alliance, "Prime specification v1.4," 2018. Powerline Intelligent Metering Evolution protocol, physical and MAC layers.

[89] INCIBE-CERT, "Guía de seguridad en protocolos industriales smart grid," tech. rep., Instituto Nacional de Ciberseguridad de España (INCIBE), 2020. Sección 4.5 DLMS/COSEM.

[90] J. Márquez and G. Rodríguez, "Análisis de seguridad del protocolo dlms/cosem en el contexto de smart grids," Master's thesis, Universidad de la República, Facultad de Ingeniería, Montevideo, Uruguay, 2020.

[91] D. V. Arteaga, "Desarrollo de aplicación android para comunicación dlms/cosem con smart meter," Master's thesis, Universidad Carlos III de Madrid, Madrid, España, 2019.

[92] —, "Security auditing of a dlms cosem smart grid," *Proceedings of Smart Grid Security Symposium*, 2018. Versión traducida al español consultada.

[93] P. Matoušek, "Analysis of dlms protocol," Dec. 2017.

[94] F. J. R. Fernández, "Implementación y análisis del protocolo dlms/cosem para la lectura de contadores inteligentes," 2021.

[95] Shenzhen Star Instrument Co., Ltd., *Manual de Operaciones: Medidor Electrónico de Energía DTS27 tres fases, cuatro hilos.* ALEMA SpA, Chile, 2023. Manual técnico.

[96] Shenzhen Star Instrument Co., Ltd., "Especificación técnica medidor ami trifásico tetrafilar multirango clase 0.5s activa – clase 2 reactiva," Technical Specification DTS27, Shenzhen Star Instrument Co., Ltd., 2023.

[97] Gurux Ltd., "Gurux dlms/cosem – open source tools for smart metering," Mar. 2025. Accessed: Mar. 1, 2025.

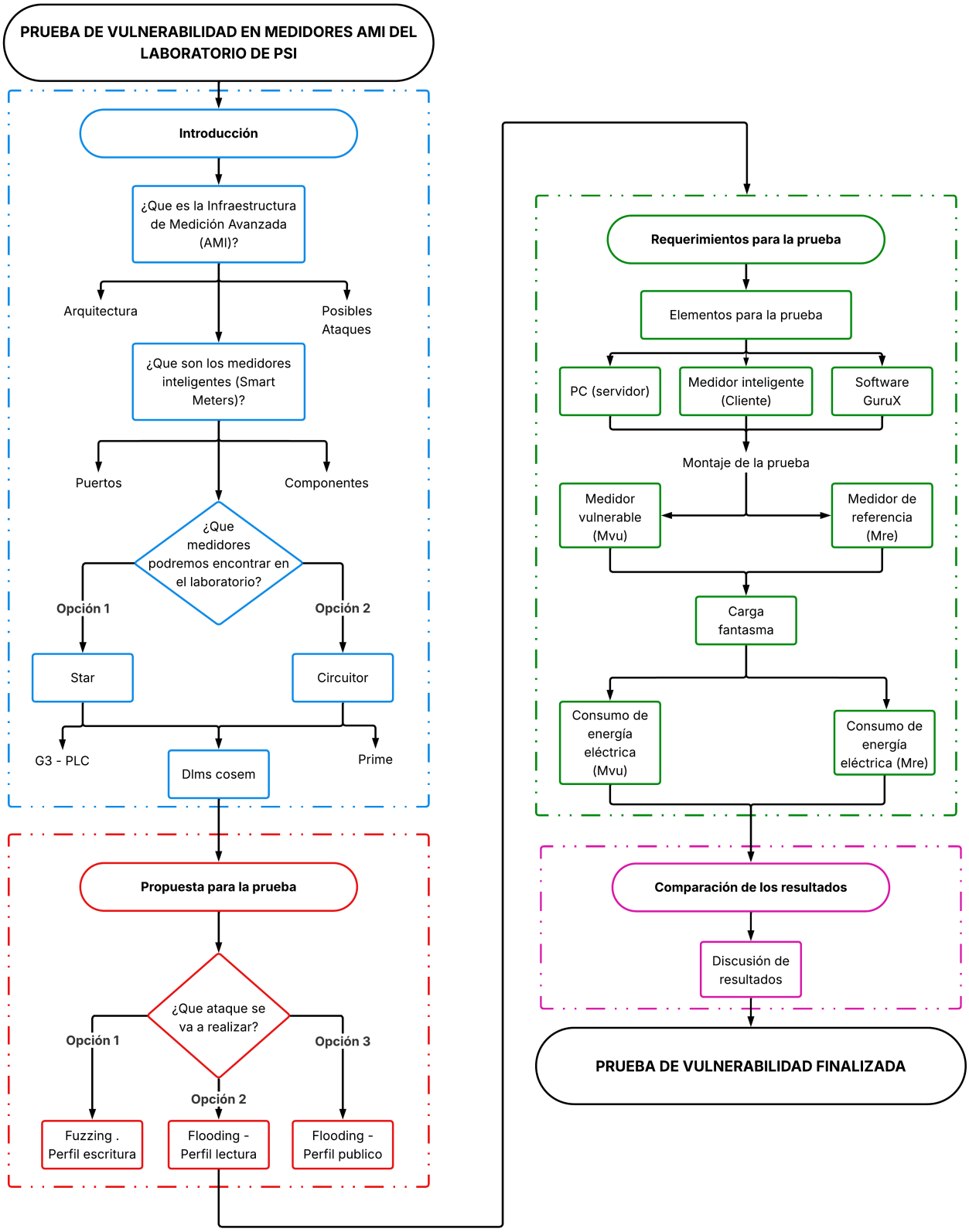
[98] Gurux Ltd., "Gurux dlms python library," Mar. 2025. Accessed: Mar. 1, 2025.

[99] I. S.A.S., "Brochure técnico carga fantasma 3f," 2025. Folleto técnico comercial.

[100] I. S.A.S., *Manual Carga Fantasma 3F.* Colombia, 2021. Versión digital del manual técnico.

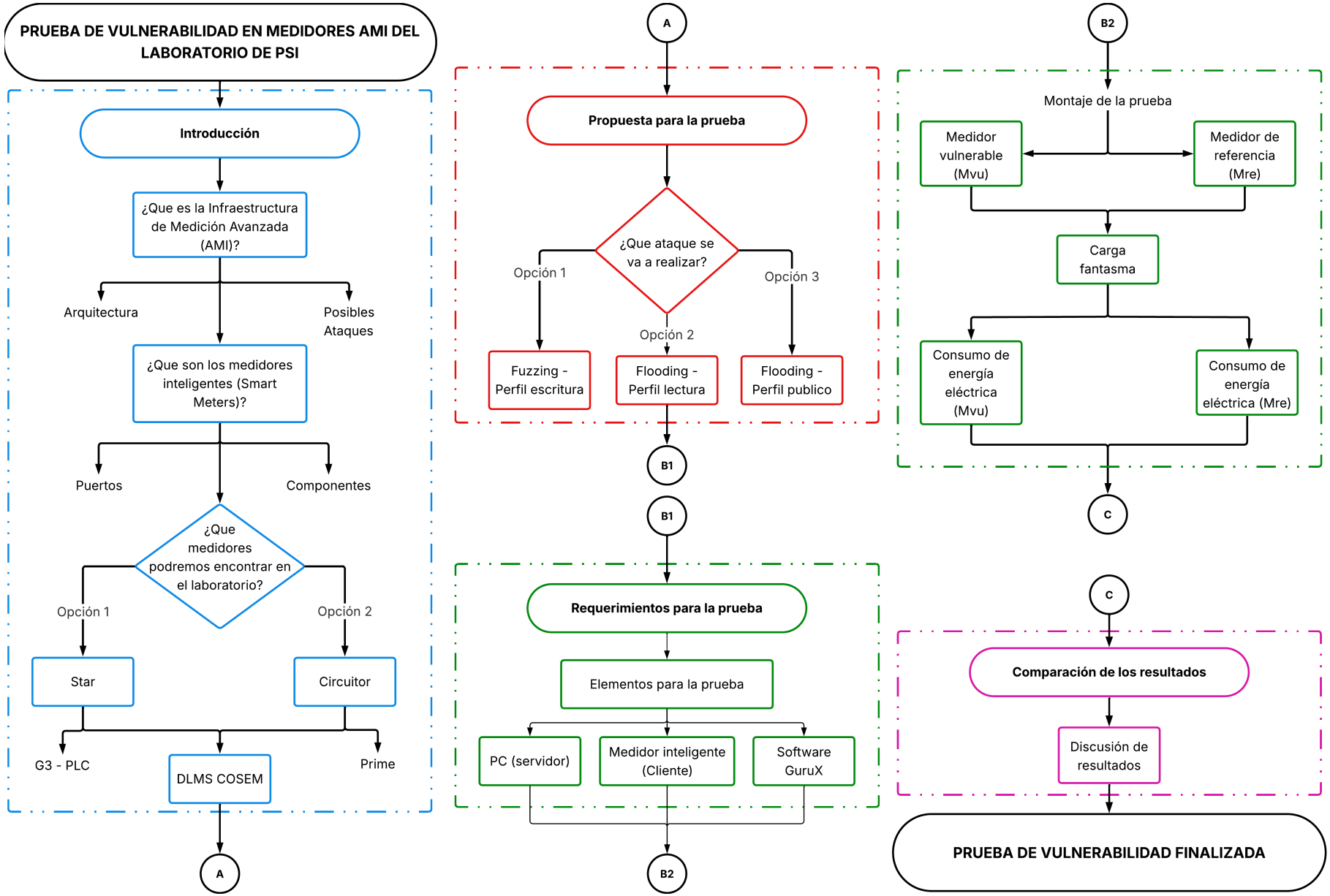
ANEXOS

Figura 5.1: Diagrama general para realizar una prueba de vulnerabilidad en medidores AMI.



Fuente: Elaboración propia

Figura 5.2: Diagrama para realizar una prueba de vulnerabilidad en medidores AMI, secciones I - A, A - B1, B1 - B2, B2 - C, C - F.



Fuente: Elaboración propia