EDUCACIÓN
SECRETARÍA DE EDUCACIÓN PÚBLICA

TECNOLÓGICO NACIONAL DE MÉXICO

INSTITUTO TECNOLÓGICO DE MORELIA

DIVISIÓN DE ESTUDIOS DE POSGRADO E INVESTIGACIÓN

DOCTORADO EN CIENCIAS DE LA INGENIERÍA

TESIS

CIBER SEGURIDAD DE TRANSACCIONES EN SISTEMAS DE MEDICIÓN INTELIGENTE USANDO CADENAS DE BLOQUES

QUE PARA OBTENER EL GRADO DE:

DOCTOR EN CIENCIAS DE LA INGENIERÍA

PRESENTA:

JUAN CARLOS OLIVARES ROJAS

DIRECTOR:

DR. ENRIQUE REYES ARCHUNDIA

CO-DIRECTOR:

DR. JOSÉ ANTONIO GUTIÉRREZ GNECCHI

MORELIA, MICHOACÁN **OCTUBRE 2021**

Instituto Tecnológico de Morelia
Subdirección Académica
División de Estudios de Posgrado e Investigación

Morelia, Michoacán, 29/SEPTIEMBRE/2021

OFICIO No. DEPI/295/2021

ASUNTO: Autorización de impresión definitiva de tesis

C. JUAN CARLOS OLIVARES ROJAS
EGRESAD DEL DOCTORADO EN CIENCIAS EN INGENIERÍA
PRESENTE.

Le comunico que el jurado designado para que obtenga el grado de **DOCTOR EN CIENCIAS EN INGENIERÍA**, ha informado a esta División de Estudios de Posgrado e Investigación, su aceptación para la impresión definitiva de su trabajo de tesis, el cual lleva por nombre: **"CIBER SEGURIDAD DE TRANSACCIONES EN SISTEMAS DE MEDICIÓN INTELIGENTE USANDO CADENAS DE BLOQUES".**

Por lo anterior se le autoriza la impresión de su trabajo, esperando que el logro del mismo sea acorde con sus aspiraciones profesionales.

SEP
SECRETARÍA DE EDUCACIÓN PÚBLICA
TECNOLÓGICO NACIONAL DE MÉXICO
INSTITUTO TECNOLÓGICO DE MORELIA
DIVISIÓN DE ESTUDIOS DE POSGRADO E INVESTIGACIÓN

A T E N T A M E N T E
Excelencia en Educación Tecnológica®
"Técnica, Progreso de México"®

C. HÉCTOR JAVIER VERGARA HERNÁNDEZ
JEFE DE LA DIVISIÓN DE ESTUDIOS DE POSGRADO E INVESTIGACIÓN

C.p. Archivo

HJVH/laa♥

Instituto Tecnológico de Morelia
Subdirección Académica
División de Estudios de Posgrado e Investigación
Doctorado en Ciencias de la Ingeniería

Morelia, Michoacán, 03/septiembre/2021

OFICIO N° DCI. 097/2021

ACTA DE REVISIÓN DE TESIS

En la ciudad de Morelia, Michoacán, siendo las **10:00** horas del día **25** de **agosto** de **2021**, se reunieron los Miembros del Comité Tutorial de Tesis, designados por el Claustro del Doctorado en Ciencias de la Ingeniería, para examinar la tesis de grado titulada:

"Ciber seguridad de transacciones en sistemas de medición inteligente usando cadenas de bloques"

Presentada por el(la) alumno(a):

M. C. JUAN CARLOS OLIVARES ROJAS, con número de Control D99120871

Aspirante al grado de:

DOCTOR EN CIENCIAS DE LA INGENIERÍA

Después de intercambiar opiniones, los miembros de la comisión manifestaron su **APROBACIÓN PARA LA IMPRESIÓN FINAL DE LA TESIS**, en virtud de que satisface los requisitos señalados por las disposiciones reglamentarias vigentes.

Presidente y Asesor:

Dr. Enrique Reyes Archundia
D. en C. en Ingeniería Eléctrica
Cédula Profesional 9350899

Secretario y Co-asesor:

Dr. José Antonio Gutiérrez Gnecchi
D. en C. en Ingeniería Electrónica
Cédula Profesional 6650058

Vocal:

Dra. Adriana del Carmen Téllez Anguiano
D. en C. en Ingeniería Mecatrónica
Cédula Profesional 6898832

Vocal:

Dr. Jaime Cerda Jacobo
PhD. en Ingeniería eléctrica y Electrónica
No. Hab. Pendiente.

Vocal:

Dr. Arturo Méndez Patiño
D. en C. en Ingeniería Electrónica
Cédula Profesional 6526003

Vocal Suplente:

Dr. Ismael Molina Moreno
D. en C. en Ingeniería Eléctrica
Cédula Profesional 11238326

C.c.p. Archivo

Abstract

Cybersecurity incidents are becoming more frequent due to the high degree of penetration that information and communication technologies have in our daily lives. One of the critical infrastructures that has benefited the most in recent years from the broad integration of technologies has been the smart grid. Smart metering systems allow, among other things, the monitoring of energy consumption and production readings that are translated into monetary transactions. The tampering and manipulation of the smart meter readings are reflected in economic losses for the utilities and loss of confidence in the end-users.

This work presents a cybersecurity architecture based on a multitier blockchain capable of adapting to smart metering systems' architecture through an edge-fog-cloud distributed computing scheme. The proposed architecture is highly scalable to the various components of smart metering systems and improves the performance of blockchains in aspects such as storage and processing. This blockchain uses its own consensus algorithm proof-of-efficiency, which allows benefiting end-users through more efficient use of their energy consumption considering the power quality, the forecast of the demand, and the support for detecting theft and energy fraud. The consensus algorithm uses the same architecture proposed to determine users' rewards through data analytics and machine learning techniques. All of this lays the foundation for a more intelligent, more transactional, and cybersecure metering system.

The architecture developed was tested to guarantee the cybersecurity of the transactions carried out in the smart metering systems. The results obtained suggest that using a blockchain architecture allows improving the cybersecurity of smart metering systems and giving end-users greater confidence in their energy transactions, being able to receive better economic incentives by making more efficient use of their energy consumption.

Dedicatoria

A Dios por sobre todas las cosas.

A mis padres Pedro y Eva por apoyarme en todo siempre. Gracias a ellos soy quien soy.

A mi esposa Cynthia Mintzy por estar siempre a mi lado ya que sin su apoyo no habría podido llegar hasta donde he llegado. Te amo corazón.

A Dalia, Juanpi y Mau por ser mi razón de ser.

A la memoria de mis familiares† que ya no están conmigo.

A todos mis familiares y amigos que siempre han sido pieza fundamental de mi desarrollo profesional y personal.

Agradecimientos

A la Secretaría de Educación Pública a través del Tecnológico Nacional de México por la autorización de la Licencia Beca-Comisión para Estudios de Posgrado que facilitó el poder dedicarme de tiempo completo para terminar mis estudios de doctorado.

Al Instituto Tecnológico de Morelia en particular al Departamento de Sistemas y Computación y a la División de Estudios de Posgrado por brindarme facilidades para terminar este trabajo.

Al Instituto de Ciencia, Tecnología e Innovación del Estado de Michoacán por brindarme apoyo económico parcial para realizar una estancia en el extranjero a través del proyecto PFCTI/ICTI/2019/B/24 “Ciber Seguridad, IoT” en la Universidad de Mánchester, Reino Unido.

A mi asesor el Dr. Enrique Reyes Archundia, por sus excelentes consejos que no solo llevaron por buen término este trabajo, sino que además me han permitido ser mejor persona. Muchas gracias por su sincera amistad y apoyo.

A mi coasesor el Dr. José Antonio Gutiérrez Gnecchi por sus sabios consejos y por todo su apoyo. Siempre estaré agradecido del apoyo en la revisión y redacción de artículos técnicos en las revistas de alto impacto que publicamos.

A mis revisores, Dra. Adriana del Carmen Téllez Anguiano, Dr. Ismael Molina Moreno, Dr. Arturo Méndez Patiño y Dr. Jaime Cerda Jacobo, por todas sus sugerencias y comentarios que permitieron enriquecer este trabajo.

Al coordinador del posgrado el Dr. Francisco Reyes Calderón por todo el apoyo administrativo para llevar por buen término este trabajo.

A todo el personal del DCI en particular a los profesores-investigadores de la línea de Tecnologías de la Electrónica.

A todos los alumnos de licenciatura y posgrado que tuve la posibilidad de dirigir y/o codirigir dentro de proyectos de investigación derivados de este trabajo doctoral.

A todos los compañeros del Doctorado en particular a mis amigos en la Línea de Tecnologías de la Electrónica: Jorge Luis, Manuel, Luis Alfredo, Javier, Gilberto†, Eduardo y Gerardo por compartir momentos de alegría y preocupaciones con su servidor.

A todos… ¡Mil Gracias!

Contenido

Abstract i
Dedicatoria ii
Agradecimientos iii
Capítulo 1 15
1.1 Antecedentes 16
1.2 Solución propuesta 20
1.3. Objetivos 21
1.3.1. Objetivo general 21
1.3.2 Objetivos específicos 21
1.4. Hipótesis 22
1.5. Justificación 22
1.6 Estado del arte 23
1.7. Aportaciones 26
1.8. Organización del contenido de la tesis 26
Capítulo 2 28
2.1 Red Eléctrica Inteligente (REI) y Sistemas de Medición Inteligente (SMI) 29
2.1.1. Sistemas Ciberfísicos en SMI 35
2.1.2. Arquitecturas de Cómputo Distribuido en REI y SMI 36
2.1.3. Radiación Electromagnética de MI 38
2.2. Ciberseguridad en REI y SMI 40
2.3 Cadena de Bloques (Blockchain) 48
2.4 Mercados Eléctricos en México 52
2.4.1. Mercados Eléctricos Transactivos 53
2.4.2. Tarifas Eléctricas en México 55
Capítulo 3 59
3.1 Conceptualización de los SMI dentro de una arquitectura borde-niebla-nube 60
3.2 Análisis de Riesgos en SMI 61
3.3 Arquitectura de una cadena de bloques multinivel para SMI 65
3.4 Algoritmo Prueba de Eficiencia (PoEf) versión 1 74
3.5 Algoritmo Prueba de Eficiencia (PoEf) versión 2: Sistema de Análisis de Datos Multinivel para SMI 78

3.6 Algoritmo Prueba de Eficiencia (PoEf) versión 3: Sistema Transactivo de Energía.....87
Capítulo 4.....98
Resultados y validación de la solución propuesta.....98
4.1. Caso 1: Arquitectura de cadena de bloques multinivel para la protección de datos.....99
4.2. Caso 2: Algoritmo de Consenso PoEf versión 1.....110
4.3. Caso 3: Plataforma de analítica de datos (PoEf versión 2).....112
4.4. Caso 4: Probando la plataforma TES (PoEf versión 3).....123
Capítulo 5.....126
Conclusiones y trabajos futuros.....126
5.1 Conclusiones.....127
5.2 Trabajos futuros.....130
5.3 Productividad lograda.....130
5.3.1 Publicaciones en Revistas JCR.....130
5.3.2 Publicaciones en revistas arbitradas e indexadas en otros índices (autor principal).....132
5.3.3 Publicaciones en revistas arbitradas e indexadas en otros índices (coautor).....134
5.3.4 Publicaciones en revistas arbitradas e indexadas aceptadas en espera de publicación (autor principal).....134
5.3.5 Capítulos de libro (autor principal).....134
5.3.6 Publicación en memorias en extenso de congreso internacional (autor principal).....135
5.3.7 Publicaciones por aparecer en memorias en extenso de congreso internacional (autor principal).....136
5.3.8 Artículos en memoria de congreso en extenso (coautor).....136
5.3.9 Publicación en revista de divulgación (autor principal).....138
5.3.10 Publicaciones en Póster (autor principal).....138
5.3.11 Colaborador de Proyectos de Investigación con Financiamiento (TecNM).....138
5.3.12 Tesis de maestría co-dirigida.....139
5.3.13 Sinodal en titulación en Licenciatura.....140
5.3.14 Asesor en residencias profesionales.....140
5.3.15 Participación como asesor en veranos de investigación.....141
5.3.16 Asesoría de alumnos de Servicio Social.....142
5.3.17 Conferencias dictadas.....142
5.3.18 Participación en proyectos de innovación.....143

Referencias.....144

Simbología, Abreviaturas y Acrónimos

Concepto	Descripción
4RI	Cuarta Revolución Industrial
AIC	Criterio de Información de Akaike
APT	Amenazas Persistentes Avanzadas
AMI	Infraestructura de Medición Avanzada
ARIMA	Modelo Autoregresivo Integrado de Promedio Móvil
ASIC	Circuitos Integrados de Aplicación Específica
BAN	Red de Área de Edificios
BD	Base de Datos
BIC	Criterio de Información Bayesiano
CA	Autoridades de Certificación
CI	Contrato Inteligente
CIAS	Confidencialidad, Integridad, Disponibilidad, Seguridad Física
CD	Concentrador de Datos
CEM	Campos Electromagnéticos
CFE	Comisión Federal de Electricidad
CONACyT	Consejo Nacional de Ciencia y Tecnología
CPP	Precio Máximo Crítico
DA	Analítica de Datos
DAG	Grafo Acíclico Dirigido
DER	Sistemas de Generación Distribuida
DDoS	Denegación Distribuida de Servicio
DLT	Libro Mayor Distribuido
DoS	Denegación de Servicio
DPoS	Prueba de Participación Distribuida
DSO	Operadores de Sistemas de Distribución
DT	Gemelos Digitales
DX	Transformación Digital

E	Electrodomésticos
EA	Analítica en el Borde
EI	Electrodomésticos Inteligentes
FA	Analítica en la Niebla
FAN	Red de Área de Campo
FC	Consenso Federado
FCC	Comisión Federal de Comunicaciones
FPGA	Matriz de Puertas Programables de Campo
G	Gauss
GUI	Interfaz Gráfica de Usuario
HAN	Red de Área Hogareña
HI	Hogar Inteligente
Hz	Herzios
IAN	Red de Área Industrial
ICS-CERT	Equipo de Respuestas ante Emergencias Cibernéticas – Sistemas de Control Industrial
IDS	Sistema de Detección de Intrusos
IED	Dispositivos Electrónicos Inteligentes
IEEE	Instituto de Ingenieros Eléctricos y Electrónicos
IoT	Internet de las Cosas
IPS	Sistema de Prevención de Intrusos
ISO	Organización de Estándares Internacionales
ISP	Proveedor de Servicios de Internet
IT	Tecnologías de la Información
JCR	Reporte de Citación de Revistas
JSON	Notación de Objetos de JavaScript
MDMS	Sistema de Gestión de Datos de Medición
MDP	Procesos de Decisión de Markov
MG	Microrred
MI	Medidor Inteligente
MitM	Hombre en el Medio
MitMo	Hombre en el Móvil

ML	Aprendizaje Máquina
MPC	Modelo de Procesamiento y Comunicaciones
MSE	Error Cuadrático Medio
NAN	Red de Área Vecinal
NIC	Tarjeta de Interfaz de Red
NIST	Instituto Nacional de Estándares y Tecnología
OMS	Sistema de Gestión de Cortes
OT	Tecnologías Operacionales
P2P	Par a Par
PBFT	Tolerancia a Fallas Práctica Bizantina
PKI	Infraestructura de Clave Pública
PLC	Comunicación por Líneas de Potencia
PNT	Pérdidas No Técnicas
PoA	Prueba de Autoridad
PoC	Prueba de Concepto
PoCW	Prueba de Trabajo Computacional
PoEf	Prueba de Eficiencia
PoET	Prueba de Tiempo Transcurrido
PoI	Prueba de Importancia
PoR	Prueba de Reputación
PoS	Prueba de Participación
PoSpace	Prueba de Espacio
PQ	Calidad de la Energía
PT	Pérdidas Técnicas
PoW	Prueba de Trabajo
RCA	Algoritmo de Consenso de Ripple
REI	Red Eléctrica Inteligente
RF	Radio Frecuencia
RL	Aprendizaje por Reforzamiento
RTP	Precio en Tiempo Real
SARIMAX	Media Móvil Integrada Autorregresiva Estacional con Variables Externas
SBC	Computadoras en una Sola Placa

SCADA	Supervisión, Control y Adquisición de Datos
SDL	Ataque sensible y de fuga de datos
SDN	Redes Definidas por Software
SEP	Sistema Eléctrico de Potencia
SFTP	Protocolo de Transferencia de Archivos Seguro
SGSI	Sistema de Gestión de Seguridad Informática
SMI	Sistema de Medición Inteligente
SO	Sistemas Operativo
SSH	Terminal Segura
TE	Energía Transactiva
TES	Sistema de Energía Transactivo
TIC	Tecnologías de la Información y Comunicaciones
TOU	Tiempo de Uso
TSO	Operadores del Sistema de Transmisión
V	Volts
VE	Vehículos Eléctricos
VPN	Red Privada Virtual
VPP	Precio Máximo Variable
W	Watts
WAN	Red de Área Extensa
W3C	Consorcio de Web Mundial Extensa

Lista de Figuras

Figura 1-1 Evolución de las revoluciones industriales [1]. 16
Figura 1-2 Cantidad de artículos técnicos de tecnologías de la 4RI en la base de datos del IEEExplore [1]. 17
Figura 1-3 Modelo conceptual de la REI basado en NIST. 18
Figura 1-4 Conceptualización de un SMI. 19
Figura 1-5 Principales vulnerabilidades en SMI. 20
Figura 2-1 Nuevas Tecnologías en la REI [49]. 30
Figura 2-2 Ciudades inteligentes [50]. 31
Figura 2-3 Principales tareas de un medidor inteligente. 32
Figura 2-4 Sistemas de Medición Inteligente. 33
Figura 2-5 Arquitectura completa de un SMI. 34
Figura 2-6 Arquitectura general de un SMI. 35
Figura 2-7 Elementos principales de un sistema ciberfísico. 36
Figura 2-8 Modelo ciberfísico de los SMI. 37
Figura 2-9 *Arquitectura de cómputo distribuida nube-niebla-borde [60].* 38
Figura 2-10 Premisas básicas de ciberseguridad. 42
Figura 2-11 Estructura de datos general básica de una cadena de bloques. 49
Figura 2-12 Modelo General de Operación de Mercados Eléctricos utilizando Cadenas de Bloques. 53
Figura 2-13 Arquitectura General de Operación de Mercados Eléctricos utilizando Criptomonedas. 54
Figura 3-1 Un SMI dentro de una arquitectura borde-niebla-nube. 60
Figura 3-2 Escenario general del funcionamiento de un SMI mostrando sus diversos puntos de falla. 63
Figura 3-3 Uso del portal del SMI. 63
Figura 3-4 Subcaso 2.1 pago de consumo eléctrico. 64
Figura 3-5 Escenario 3 de comunicación de lecturas de medición de los MI a través del SMI. 64
Figura 3-6 Arquitectura propuesta basada en las cuatro áreas elementales deAMI. 66
Figura 3-7 Almacenamiento de datos general de la arquitectura de cadena de bloques propuestas. 67
Figura 3-8 Estructura de datos Blockchain implementada en el nivel HAN. 68
Figura 3-9 Estructura de datos de la cadena de bloques implementada en el nivel NAN. 69
Figura 3-10 Ejemplo de una prosa legal. 70
Figura 3-11 Estructura de datos de la cadena de bloques implementada a nivel FAN / WAN. 71
Figura 3-12 El proceso de limpieza de un nodo de la cadena de bloques. 72
Figura 3-13 Proceso de adición de nuevos nodos. 73
Figura 3-14 La estructura de datos completa de Blockchain en el último nivel. 74
Figura 3-15 Diagrama de alto nivel de la arquitectura propuesta. 79
Figura 3-16 El aprendizaje por reforzamiento en la arquitectura propuesta. 81
Figura 3-17 Arquitectura para pronóstico de Consumo y Producción. 82
Figura 3-18 Arquitectura para clasificación y predicción de calidad de la energía. 84
Figura 3-19 Arquitectura para predicción de robo de energía. 86
Figura 3-20 Modelo Propuesto de Mercados Eléctrico Minorista Transactivo. 88

Figura 3-21 Interfaces de la plataforma de energía transactiva propuesta. 89
Figura 3-22 Interacciones de la plataforma de energía transactiva propuesta. 89
Figura 3-23 La Arquitectura de Sistema de Energía Transactiva usando SMI y cadena de bloques. 90
Figura 3-24 Arquitectura TES en profundidad. 91
Figura 3-25 Energía transactiva en un blockchain multi-nivel. 93
Figura 3-26 Flujo principal del TES propuesto. 94
Figura 4-1 La arquitectura implementada para las pruebas. 99
Figura 4-2 Arquitectura de hardware del MI. 100
Figura 4-3 Captura de pantallas del portal de medición modificado. 100
Figura 4-4 Diagrama de bloques de la implementación de Blockchain en NAN. 101
Figura 4-5 Escenario de ataque de precio falso. 103
Figura 4-6 Diagrama de Casos de Uso de un DT Framework Controller. 104
Figura 4-7 Arquitectura de un prototipo DT para SMI en SH. 105
Figura 4-8 Escenario de pruebas de manipulación. 109
Figura 4-9 La predicción de energía de las transacciones usando PoEf versión 2. 110
Figura 4-10 Consumo de medidores inteligentes por día. El eje x representa los días y el eje y representa el consumo por día en kW/h. 111
Figura 4-11 Predicción de producción de energía en medidor #2. 114
Figura 4-12 Lectura de consume de energía del medidor inteligente #1. 115
Figura 4-13 Lecturas de producción de energía del medidor inteligente #2. 115
Figura 4-14 Porcentaje de transacciones recompesadas fuera de verano. 124
Figura 4-15 Porcentaje de transacciones recompensadas en verano. 124

Lista de Tablas

Tabla 1-1 Cuadro Comparativo de trabajos relacionados 24
Tabla 2-1 Tiempo de Exposición. 40
Tabla 2-2 Niveles máximos de RF en algunos dispositivos. 41
Tabla 2-3 Ejemplo de riesgos en la REI. 44
Tabla 2-4 Ejemplos de impacto de riesgos en la REI. 44
Tabla 2-5 Ejemplo de políticas de ciberseguridad en REI. 45
Tabla 2-6 Algotimos de consensos más importantes en la literatura. 50
Tabla 2-7 Estructura de tarifas eléctricas por temperatura. 56
Tabla 2-8 Ejemplo de tarifas escalonadas y costos de energía en tarifa 1D en Región Centro Occidente. 56
Tabla 2-9 Tarifas eléctricas fuera de verano. 56
Tabla 2-10 Tarifas eléctricas en verano. 57
Tabla 2-11 Límte de alto consumo 57
Tabla 2-12 Tarifas por regiones y Estados. 57
Tabla 3-1 Calificación de riesgo para cada premisa de ciberseguridad. 61
Tabla 3-2 Marcador Total para evaluación de riesgo de un recurso. 62
Tabla 3-3 Clases de Eventos de Calidad de la Energía. 85
Tabla 4-1 Resultados del escenario de manipulación. 109
Tabla 4-2 Transacciones de consumo de medidores inteligentes, facturación y recompensas en cadenas de bloques NAN. 112
Tabla 4-3 Consumo de concentradores de datos, facturación y transacciones recompensadas en blockchain. 112
Tabla 4-4 Base de datos del medidor inteligente para grabar registros de Consumo y Producción. 113
Tabla 4-5 Base de datos del CD parar grabación del consumo y producción de energía en NAN. 113
Tabla 4-6 Rangos de aprendizaje en la aplicación de análitica de datos en el pronóstico de consumo/producción. 116
Tabla 4-7 Base de datos SM para clasificar eventos de calidad de la energía. 117
Tabla 4-8 Tabla de IDs representando eventos de calidad de la energía. 118
Tabla 4-9 Vector de estado representando eventos de calidad de la energía. 118
Tabla 4-10 Base de datos de clases en SM. 119
Tabla 4-11 Base de datos en el CD con una clasificaciín de eventos de calidad de la energía en HAN. 119
Tabla 4-12 Clasificación de eventos de calidad de la energía en CD. 119
Tabla 4-13 Matriz de confusión de clasificación eventos de calidad de la energía. 120
Tabla 4-14 Tasas de aprendizaje en Clasificación de Eventos calidad de la energía. 120
Tabla 4-15 Base de datos del MI para registro de predicciones de Consumo y Producción. 121
Tabla 4-16 Base de datos CD database para grabación de predicciones de consumo y producción en NAN. 121
Tabla 4-17 Resultados CD en aplicación analítica de datos para predicción de robo de energía... 122
Tabla 4-18 Matriz de confusion de detección de robo de energía. 122

Tabla 4-19 Tasas de aprendizaje en Clasificación de Robo de Energía. 123
Tabla 4-20 Comparativa usando TES en tarifas mexicanas. 125
Tabla 5-1 Resultados principales de publicaciones derivadas de este trabajo. 131
Tabla 5-2 Resultados principales de formación de recursos humanos 140

Lista de Algoritmos

Algoritmo 1 Proof-of-Efficiency Version 1 básica 76
Algoritmo 2 Pronóstico de Consumo y Producción de Energía. 83
Algoritmo 3 Clasificador usando Árbol de Decisión 85
Algoritmo 4 Clasificador de predicción de robo de Energía 87
Algoritmo 5 Prueba de Eficiencia Versión 3 94
Algoritmo 6 Ejemplo de CI en la plataforma TES propuesta 97

Lista de Ecuaciones

Ecuación 1 Fórmula empírica del riesgo 42
Ecuación 2 Definición de Energía Transactiva. 91
Ecuación 3 Costos netos 94
Ecuación 4 Costos Finales 95

Capítulo 1
Introducción

En este capítulo se presentan los antecedentes relacionados con la Ciber Seguridad de Transacciones en Sistemas de Medición Inteligente, partiendo de la descripción de la problemática a resolver, mostrando los objetivos de este trabajo, sus hipótesis, así como mostrando la propuesta de solución del problema comparándola críticamente con los trabajos relacionados existentes en la literatura. La revisión del estado del arte permite mostrar las aportaciones y contribuciones de este trabajo en el ámbito científico, tecnológico, social y económico.

1.1 Antecedentes

Actualmente estamos viviendo en una era en constante cambio derivado de diversas tecnologías que están originando la cuarta revolución industrial (4RI). Estas nuevas tecnologías son diversas, pero podemos englobarlas dentro de los sistemas ciberfísicos, en donde los sistemas físicos se interrelacionan directamente con los sistemas virtuales (ver Figura **1-1**).

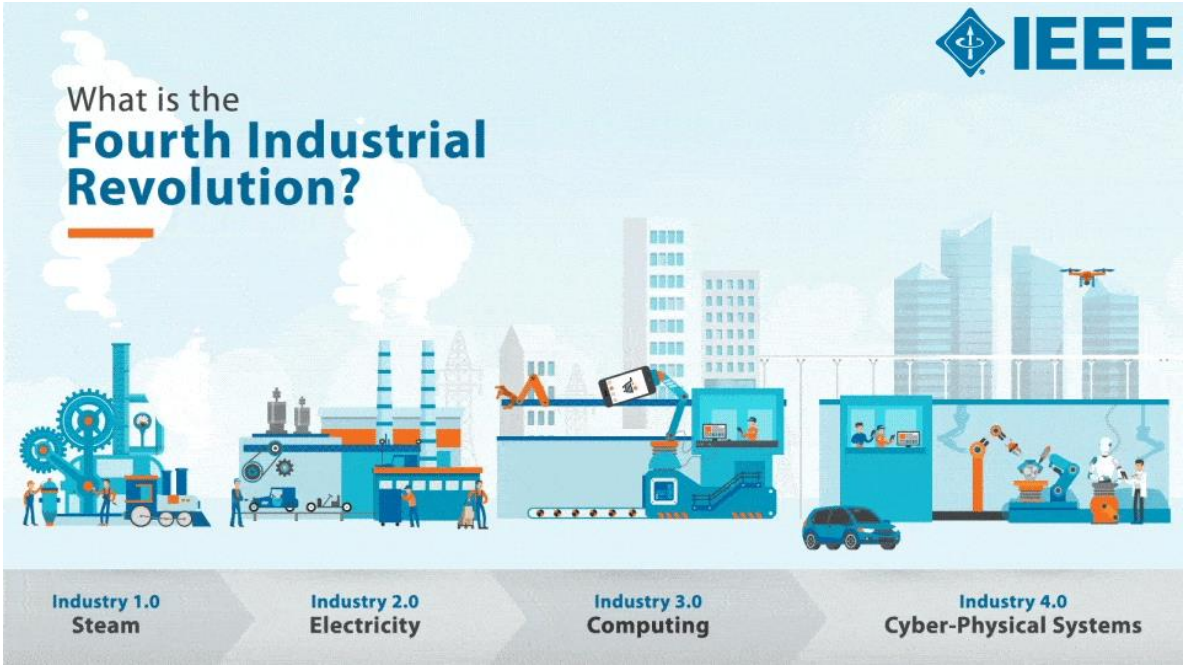

Figura 1-1 *Evolución de las revoluciones industriales [1].*

Entre algunas de las tecnologías de la 4RI se encuentran: el Intenet de las Cosas (IoT, por sus siglas en inglés), cómputo en la nube, impresión en 3D, robótica, realidad aumentada, cadena de bloques (*blockchain*), entre otras [1]. En la Figura **1-2**, se muestran las tecnologías de las 4RI más citadas en la Base de Datos (BD) del IEEE (Instituto de Ingenieros Eléctricos y Electrónicos).

Todas las tecnologías de la 4RI tienen como objetivo común lograr mejorar la calidad de vida de las personas y han permeado a prácticamente todas las actividades del quehacer humano, motivo por el cual a esta etapa de nuestra humanidad se la ha empezado a denominar como la era de la Transformación Digital (DX, por sus siglas en inglés) [2].

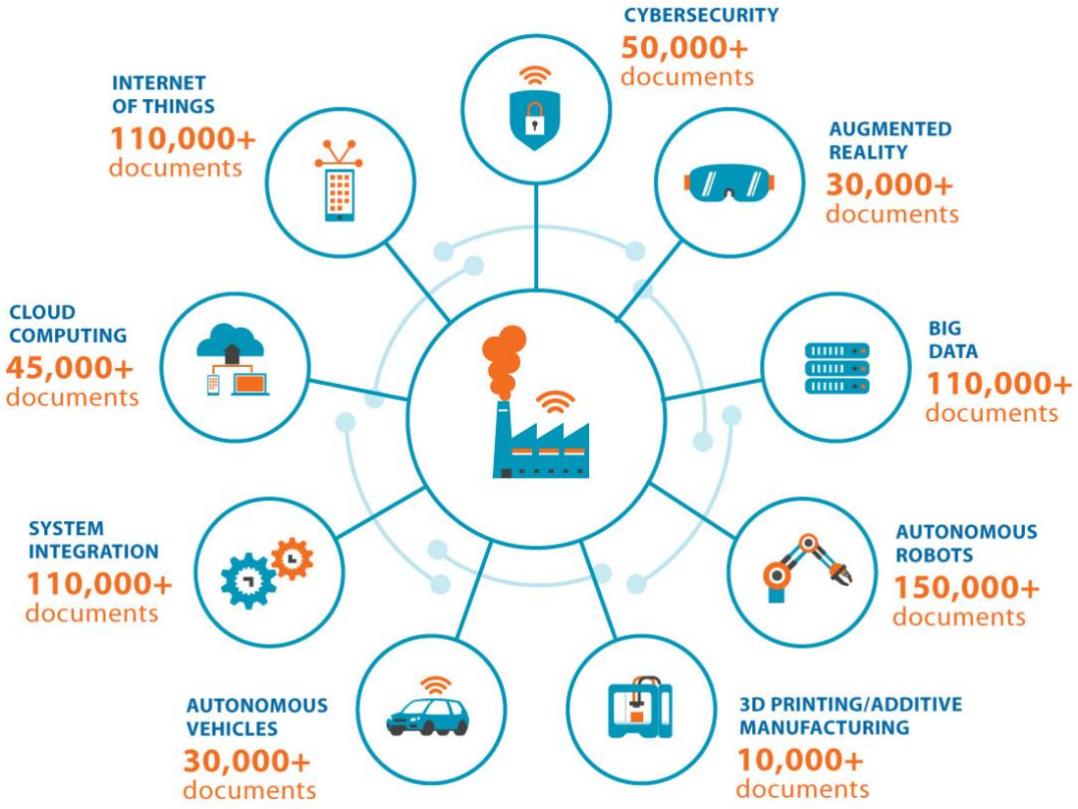

Figura 1-2 *Cantidad de artículos técnicos de tecnologías de la 4RI en la base de datos del IEEExplore [1].*

Una de las áreas de mayor transformación ha sido la red eléctrica; la cual tenía demasiados años sin sufrir modificaciones. El uso de las tecnologías de la 4RI ha traido consigo a que la red eléctrica se haya vuelto más inteligente, motivo por el cual ha pasado a denominarse como Red Eléctrica Inteligente (REI). La REI ha permitido no solo automatizar procesos y operaciones de los sistemas eléctricos de potencia, sino que a su vez ha permitido que el suministro de energía eléctrica sea más confiable, barato y sobre todo menos contaminante al fomentar el uso energías limpias [3]. En la Figura **1-3** se muestra el modelo conceptual de la REI propuesta por el Instituto Nacional de Estándares y Tecnologías (NIST, por sus siglas en inglés) [4], en donde se puede observar que además de los flujos de electricidad (representados por líneas azules) y de los dominios comunes de Generación, Transmisión, Distribución y Consumo (clientes), existen flujos de comunicación de información segura (representados por líneas punteadas rojas) y otros dominios como la operación, los mercados eléctricos y los proveedores de servicios.

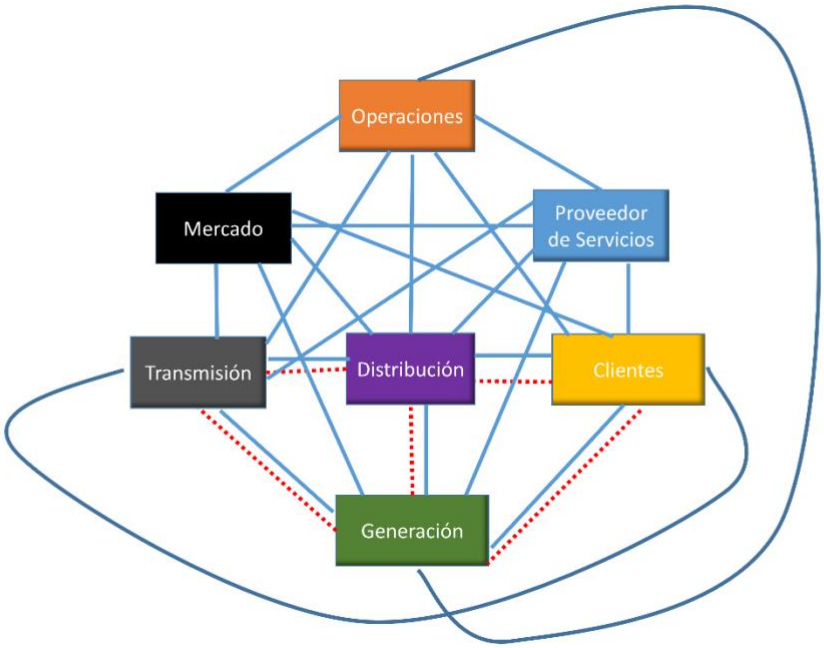

Figura 1-3 *Modelo conceptual de la REI basado en NIST.*

El concepto de la REI se empezó a manejar hace aproximadamente 15 años (finales de la década de los 2000) y vino de la mano del uso de los denominados medidores inteligentes (MI). Los MI evolucionan del medidor electrónico al agregarle capacidades de comunicaciones y procesamiento al sistema embebido del medidor, convirtiéndose en un dispositivo de IoT bastante robusto. Los MI permiten monitorear el consumo de energía eléctrica en todo momento, además de automatizar operaciones como los procesos de facturación así como los cortes y reconexiones del servicio sin la intervención manual de operadores [5]. Para ello, se requiere además de los MI de un conjunto de elementos denominado como Sistemas de Medición Inteligente (SMI) siendo la Infraestructura de Medición Avanzada (AMI, por sus siglas en inglés), la implementación mejor conocida. Recientemente se han agregado nuevas funciones entre las que se encuentran la medición de energía produciva a través de sistemas de generación distribuida (DER, por sus siglas en inglés), el manejo de tarifas eléctricas por uso horario y en tiempo real, así como la integración con sistemas de gestión de energía y de respuesta a la demanda [6]. En la Figura **1-4** se muestra de manera general un SMI (en el Capítulo 2 se ahonda más en este punto).

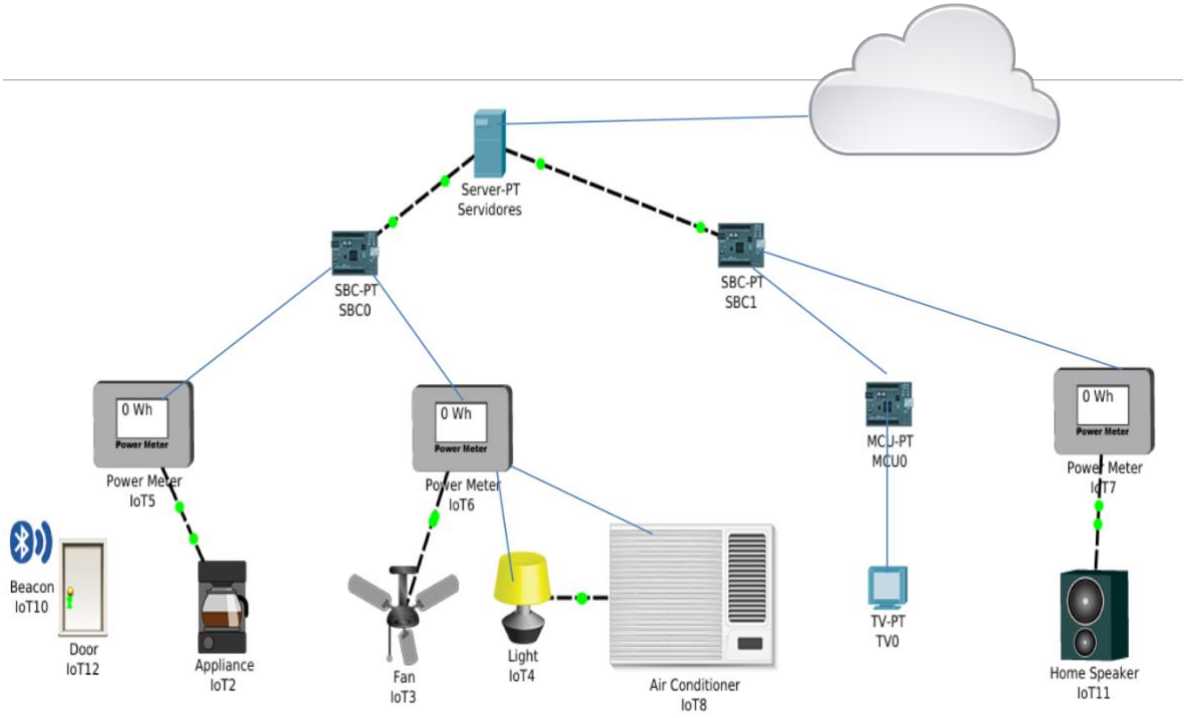

Figura 1-4 *Conceptualización de un SMI.*

Sin embargo, a pesar de las enormes ventajas que traen consigo la REI y los SMI también se presentan nuevos retos y oportunidades derivado del uso de las tecnologías de la 4RI, uno de ellos, la ciberseguridad. De acuerdo con la Comisión Federal de Eléctricidad (CFE) [7] se estima el nivel de pérdidas no técnicas (errores de medición, facturación, robo y fraude de energía eléctrica) a nivel nacional en un 25.2%.

Aunque los MI y los SMI presentan esquemas de ciberseguridad para la confidencialidad, integridad y disponibilidad de los datos, nunca es suficiente debido al incremento de las amenazas y vulnerabilidades que presenta cualquier sistema informático.

En la Figura **1-5** se muestra las diversas vulnerabilidades que se presentan en los SMI. Se puede observar que los SMI son sistemas complejos y muy heterogéneos por lo que las vulnerabilidades se presentan de forma muy diversa y en diversos puntos de su infraestructura. Por ejemplo, los mismos dispositivos eléctricos que ahora tienen capacidades de comunicación (dispositivos IoT) en el hogar pueden inducir fallas de ciberseguridad. Por otra parte, los MI que poseen capacidades de cómputo y almacenamiento son una de los principales activos de información en tratar de ser atacados. Además de lo anterior, se pueden

presentar fallas de ciberseguridad en los medios de transmisión de datos y en la infraestructura tecnológica de las empresas eléctricas.

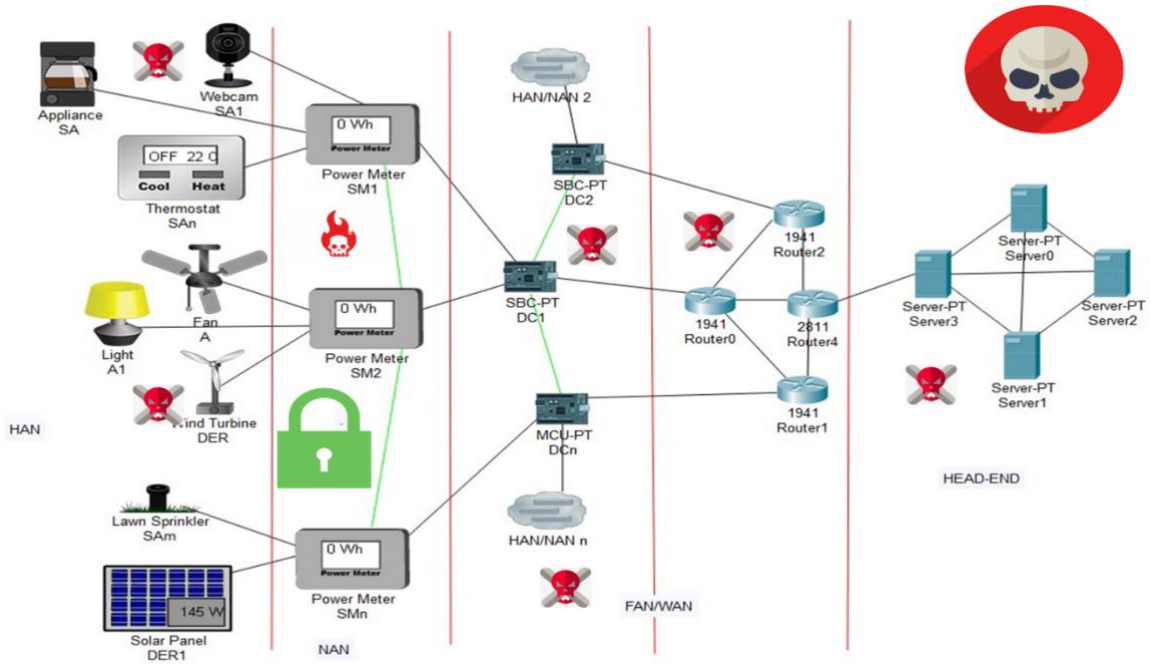

Figura 1-5 *Principales vulnerabilidades en SMI.*

1.2 Solución propuesta

La ciberseguridad es un área bastante estudiada en la literatura y en el campo de las REI y SMI no es nuevo. Existen diversos enfoques utilizados en tratar de garantizar la protección de los activos de información, desde el uso de criptografía para cifrar y descifrar la información, hasta mecanismos de análisis de tráfico en redes de datos como lo son los cortafuegos (*firewalls*), por mencionar algunos.

En los últimos años, ha surgido el concepto de *blockchain* (cadenas de bloques) que trata sobre la combinación de diversas tecnologías para garantizar confianza en las transacciones de cualquier sistema informático [8]. Entre los principales componentes de la cadena de bloques se encuentran las técnicas de criptografía asimétrica para el manejo de firmas digitales para garantizar la identidad de los usuarios, el manejo de funciones de resumen (*hash*) para garantizar integridad de los datos, así como esquemas novedosos de validación de transacciones denominados algoritmos de consenso [9], entre otros.

Como se puede apreciar, el uso de cadenas de bloque provee enormes ventajas que permiten garantizar la confidencialidad, integridad y disponibilidad de los datos en sistemas de transacciones, por lo que su uso en la REI se ha ido incrementando en los últimos años [10]. Sin embargo, el uso de cadena de bloques por si solo presenta algunos retos que aunados a los retos presentes en los SMI hace necesario tomar en cuenta nuevas consideraciones referentes a la ciberseguridad y al desempeño de las cadenas de bloques.

En este trabajo doctoral se propone un SMI transactivo utilizando una cadena de bloques multinivel, el cual permite garantizar la ciberseguridad de los datos de medición de consumo y producción de energía eléctrica. El trabajo que se propone utiliza para la validación de transacciones, un algoritmo de consenso propio denominado *Proof-of-Efficiency* (PoEf, prueba de eficiencia) basado en una plataforma de analítica de datos multinivel que al igual que la arquitectura de cadena de bloques propuesta, aprovecha los esquemas de cómputo distribuido de borde-niebla-nube. Los resultados de la analítica de datos además de validar transacciones de consumo/producción de energía eléctrica, permiten recompensar a los usuarios que hacen un uso más eficiente de su consumo y producción de energía eléctrica con base en factores de calidad de la energía, esto trae consigo un modelo transactivo de energía beneficioso para los usuarios finales y la empresa eléctrica gubernamental al eliminar subsidios y reducir costos en ambas partes. Finalmente, la solución propuesta fue probada a través de diversos ataques pertinentes a las cadenas de bloques utilizando un esquema de gemelos digitales.

1.3. Objetivos

1.3.1. Objetivo general

El objetivo general de este trabajo consiste en: "*Mejorar la seguridad de las transacciones en los Sistemas de Medición Inteligente al implementar un mecanismo de cadenas de bloques que permitan garantizar la integridad, confidencialidad y disponibilidad de la información que garanticen confianza entre los usuarios y la empresa eléctrica"*.

1.3.2 Objetivos específicos

- Estudio de vulnerabilidades de los SMI enfocados en: protocolos de comunicación (alámbricos e inalámbricos), hardware y software.

- Diseño, desarrollo, implementación y simulación de un SMI de energía eléctrica con capacidad de comunicación bidireccional tanto cableada como inalámbrica.

- Estudio de los diversos mecanismos de cadenas de bloques para brindar confianza en transacciones de consumo energético.

- Diseño, desarrollo e implementación de un mecanismo de cadena de bloques en MI que garantice la seguridad de la información en los SMI.

- Realización de diversas pruebas de penetración para verificar y validar la seguridad de la solución implementada.

1.4. Hipótesis

El modelo de un sistema de cadena de bloques en SMI garantiza una mayor ciberseguridad en las transacciones de consumo/producción de energía eléctrica al prevenir distintas amenazas como lo es la manipulación de los datos de medición.

1.5. Justificación

Según la firma Fortune Business Insights [11], el tamaño del mercado mundial de MI se situó en 16.39 mil millones de dólares estadounidenses en 2018 y se prevé que alcance los 30.19 mil millones de dólares estadounidenses para 2026. De manera particular el crecimiento se ha dado en las regiones de Norteamérica, Europa y Asia-Pacífico. De los diversos sectores de uso de energía, el sector de usuario residencial abarca el 86%. En el caso latinoamericano, las tendencias han sido menores que en otras regiones, pero el crecimiento ha sido considerable en países como Brasil, Colombia, Chile y México. En México, desde 2014 la compra de nuevos medidores se hace considerando la tecnología AMI, en la cual se tienen más de 5 millones de MI con estas características; sin embargo, son pocos los proyectos implementados debido al alto costo de la infraestructura de telecomunicaciones y de Tecnologías de la Información y Comunicaciones (TIC) [7]. Así, el mercado de los SMI es muy importante en el aspecto financiero y es considerado como la parte fundamental de la REI debido a que es la parte más visible para los usuarios finales y está directamente relacionada con la parte de facturación y otros servicios. Además, la infraestructura de los SMI pasa por prácticamente todos los dominios de la REI por lo que su interconexión y monitoreo es vital para las empresas eléctricas.

Los errores en las lecturas de medición, el fraude y robo de energía, entran en la categoría de pérdidas no técnicas, las cuales se estiman en grandes pérdidas económicas para las empresas de servicios públicos. En México, de acuerdo con la CFE, presentó pérdidas por $1,407

millones de pesos en 2018 debido a pérdidas no técnicas de energía eléctrica. De hecho, durante el 2018 la CFE registró 12,936 quejas de usuarios que argumentaba un cobro excesivo o no relacionado a su consumo eléctrico habitual [12]. Con la cada vez más creciente integración de las TIC en los MI y SMI, las pérdidas no técnicas de energía se han vuelto una nueva preocupación debido a los riesgos de ciberseguridad. De acuerdo al Departamento de Defensa de los Estados Unidos de América, en el 2018 hubo más 4,300 ciber ataques a la infraestuctura de la REI en Norteamérica [13]. Por otra parte, en [11] sugiere que los ingresos globales de la tecnología blockchain experimentarán un crecimiento masivo en los próximos años, y se espera que el mercado suba a más de 39 mil millones de dólares para 2025. El sector financiero ha sido uno de los más rápidos en invertir en cadenas de bloques, con más de 60% del valor de mercado de la tecnología concentrado en este campo. Dentro del área de la REI, el 90% de los proyectos se encuentran dentro del área de distribución [14]. Dentro de los proyectos de cadenas de bloque del área de consumo 90% se encuentran dentro del área de energía transactiva y 10% en el área de medición.

Desde el punto social, el uso de sistemas confiables de medición de energía eléctrica contribuirá a un uso más eficiente de la energía, así como a una mejor forma de compartir energía renovable de forma segura y barata entre los usuarios finales y la empresa eléctrica.

Derivado de los puntos anteriores, se visualiza que la arquitectura que se propone para SMI no sólo es válida desde el punto de vista económico y social, sino también desde el punto de vista científico al presentar mejoras en el estado del arte, el cual se describe a continuación en la siguiente sección.

1.6 Estado del arte

En la literatura científica y en ambientes de desarrollo e innovación tecnológica, el estudio de la ciberseguridad en la REI y otras infraestructuras críticas ha sido ampliamente analizado desde hace varios años. Desde técnicas de criptografía robustas y ligeras para MI y otros dispositivos electrónicos inteligentes (IED, por sus siglas en inglés) hasta Sistemas de Prevención y Detección de Intrusos (IPS/IDS). En general el uso de técnicas de ciberseguridad combinadas ha demostrado ser mucho más eficaz que utilizar un solo mecanismo de seguridad. Por este motivo, el uso de las cadenas de bloque ha proliferando en los últimos años, como medio para garantizar seguridad y confianza en sistemas transaccionales particularmente donde existe flujo de dinero [15].

A continuación, se describen la revisión de la literatura del estado del arte para fianlizar con un cuadro comparativo que se muestra en la Tabla **1-1**. En donde: T = Trabajo, C = Características, P = Permisos, AC = Algoritmo de Consenso, Pr = Procesamiento, CI = Contrato Inteligente, TC = Tipo de Cadena, O = Otros.

Tabla 1-1 *Cuadro Comparativo de trabajos relacionados*

T	C	P	AC	Pr	CI	TC	O
[16]	Mercados de energía	Privado con permisos	Proof-of-concept (PoC)	Nube	S	Simple	Múltiples Firmas
[18]	Mercados de energía	Privado con permisos	Proof-of-Stake (PoS)	Nube	S	Simple	
[19]	Privacidad Precios	Privado/Público	PoW (Proof-of-Work)	Nube	N	Doble	
[23]	Seguridad REI	Privado con Permisos	PoW	Nube	N	Simple	Diferentes estructuras de datos de CB
[24]	Criptomonedas en General	Público/Privado	Doble: Proof-of-reputation (PoR) y Proof-of-ComputingWork (PoCW)	Nube	N	Multinivel	BlockDAG
[25]	Auditoría Forense	Privada con y sin permisos	PoS	Nube	N	Simple	Fragmentación Datos
[26]	Arquitectura Cómputo Distribuido	Pública con y sin permisos	PoW	Nube/Niebla	N	Doble	SDN
[27]	Detección de Malware	Privado/Público	Híbrido: PoW/PoS	Nube	Parcial	Doble	Prosa Legal
[29]	Smart Home Comercialización	Público	PoW	Nube	S	Simple	Dispositios IoT
[32]	Comercialización	Público	PoW	Nube/ Borde	S	Simple	Hardware adicional
Propuesta	Seguridad Transacciones SMI	Privado con y sin Permisos	Híbrido por cada nivel. Proof-of-Efficiency	Nube/Niebla/ IoT (medidores y dispositivos)	Parcial (Prosa)	Multinivel	Interconexión de CB Externas Fragmentación Datos

En [16] se muestra Priwatt, el cual es un sistema de comercialización de energía a través del uso de esquemas de blockchain, multi-firmas y flujos de mensajes anónimos.

Existes diversos trabajos enfocados en generar criptomonedas y esquemas financieros para REI, como en [17] en donde muestra NRGcoin. La cual es una criptomoneda que ayuda a la comercialización de energía limpia usando la infraestructura de la cadena de bloques. Otra implementación es Helios que define una criptomoneda y un protocolo de consenso descentralizado [18].

En [19] y [20] se presenta un esquema ligero para preservar y comparticir privacidad con un blockchain doble para sistemas de precios inteligentes en REI.

El esquema de manejo de múltiples cadenas se está haciendo cada vez más común en la literatura [21], [22].

Otros tipos de trabajo radica en el monitoreo de las operaciones de REI, como por ejemplo en GridMonitoring [23]. En dicho trabajo se muestra una implementación de un blockchain para protección de los datos en REI.

La referencia [24], muestra la implementación Phantom, la cual es una cadena de bloques que permite la inclusión de diversos algoritmos de consenso en diferentes niveles.

En [25] se muestra la implementación de libros mayores de contabilidad fragmentados (parciales) y completos; todo esto con el objeto de tener una cadena de bloques más eficiente para el manejo de diversas entidades y dispositivos, particularmente de vehículos eléctricos.

En [26] se presenta una propuesta de arquitectura de blockchain basada en la nube y en el nuevo concepto de cómputo en niebla (*fog computing*). En esta arquitectura las operaciones de la cadena de bloques se encuentran en la nube. La información fluye desde la capa de dispositivos hacia la nube a través de la capa de niebla. En la capa de niebla utilizando el paradigma de Redes Definidas por Software (SDN, por sus siglas en inglés) se forma una especie de cadena de bloques para problemas más concretos.

En [27] se muestra la implementación de un mecanismo de cadena de bloques para la detección de *Malware* en dispositivos móviles. Lo novedoso de esta propuesta es que permite la interconexión de otras cadenas públicas a través de un consorcio de cadenas de bloques. Otras implementaciones de cadenas de bloque en consorio para REI se muestra en [28].

Muchas implementaciones de cadenas de bloques se han implementado en entornos hogareños en combinación con mecanismos de seguridad y privacidad de la información [29],[30], y [31].

Existen diversas implementaciones comerciales de cadenas de bloques dentro del área de la REI y SMI [32], [33], y [34], particularmente enfocadas en energía transactiva de par a par.

Existe una gran cantidad de patentes del área de cadenas de bloques para REI y SMI, particularmente de China, Corea del Sur, Estados Unidos, entre otros [35], [36], [37], [38], [39], [40] y [41]; enfocados principalmente en sistemas transactivos de energía.

1.7. Aportaciones

Como pudo observarse en la sección anterior, aunque existe una gran cantidad de investigación aplicada al campo de las cadenas de bloques en la REI, son pocos los trabajos centrados en SMI utilizados para garantizar la ciberseguridad de las transacciones de consumo/producción eléctrica. Este trabajo doctoral aporta principalmente lo siguiente:

1. Una arquitectura de cadena de bloques multinivel adaptable a los SMI para garantizar ciberseguridad en las transacciones de consumo/producción de energía eléctrica [42].
2. La utilización de la arquitectura multinivel para el desarrollo de analítica de datos en SMI aplicados dentro del algoritmo de consenso para la detección de anomalías, pronóstico y mejora en la calidad de la energía [43].
3. La propuesta de un modelo transactivo de energía simple que combina las dos aportaciones previas para SMI [44].
4. La utilización de pruebas de ciberseguridad a la infraestructura utilizando una implementación sencilla de gemelos digitales [45].

Adicionalmente se proponen dos aportaciones secundarias importantes:

1. Estudio básico del impacto de los SMI en el campo de la salud [46].
2. La utilización de una metodología de ciber higiene para garantizar la adecuada protección de los SMI y de la REI en general [47].

Todas estas aportaciones se vieron refljeadas en publicaciones indizadas de alto impacto en el índice de Reporte de Citación de Revistas (JCR, por sus siglas en ingles) y en revista del Consejo Nacional de Ciencia y Tecnología (CONACyT). Además, se realizaron otras publicaciones en revistras arbitradas, indizas y conferencias internacionales. Todas estas aportaciones se describen a mayor detalle en el capítulo 5.

1.8. Organización del contenido de la tesis

En el Capítulo 2 se presenta los fundamentos teóricos científicos y tecnológicos que son necesarios para entender este trabajo y que le dan su sustento. El Capítulo 3 sienta las bases de la arquitectura implementada de forma detallada describiendo su análisis, diseño e implementación. El Capítulo 4 muestra los resultados obtenidos de probar y validar la arquitectura propuesta, realizando una discusión crítica de los resultados. Finalmente, el

Capítulo 5 muestra las conclusiones de este trabajo, así como determina trabajos futuros y remarcar las principales aportaciones científicas y tecnológicas alcanzadas.

Capítulo 2
Marco Téorico

En este capítulo se presentan la teoría y los datos importantes respecto a las redes eléctricas inteligentes, sistemas de medición inteligente, ciberseguridad, cadena de bloques, así como otros conceptos que le dan sustento técnico científico a este trabajo**.**

2.1 Red Eléctrica Inteligente (REI) y Sistemas de Medición Inteligente (SMI)

La electricidad es una comodidad esencial para soportar nuestras actividades diarias. Los sistemas de energía, particularmente el Sistema Eléctrico de Potencia (SEP), han sido el motor de la Industria y de prácticamente todo el quehacer humano. El SEP está conformado por toda la infraestructura necesaria para la generación, transmisión, distribución y consumo de energía eléctrica. La generación de electricidad puede verse como un sistema complejo multienergético: gas, carbón, petróleo, nuclear, etc.; es decir, se depende de diversas fuentes y costos para generar electricidad; mientras que las redes de transmisión y distribución se encargan de hacer llegar el suministro eléctrico a donde se necesita.

Los procesos de generación, transmisión y distribución de energía eléctrica presentan pérdidas de energía clasificadas como Pérdidas Técnicas (PT) y Pérdidas No Técnicas (PNT) de Energía. Las PT se deben a la pérdida de energía de forma física al realizar los procesos de generación, transmisión y distribución; y se consideran hasta cierto punto normales. Por otra parte, las PNT se refieren a fenómenos más de índole humano como son los errores de medición, errores de facturación, robo y fraude de energía.

Las Redes Eléctricas de los SEP han estado presentes desde hace más de 125 años y se han tratado de ir mejorando para lograr una mejor generación, transmisión, distribución y consumo de energía que los haga más eficientes y amigables para el medio ambiente. En los últimos años con la inclusión de las TICs la red eléctrica tradicional se ha vuelto inteligente para ayudar en los procesos de generación, transmisión, distribución y consumo de energía eléctrica. Aunque la demanda de energía eléctrica sigue creciendo a nivel mundial, en general el consumo de energía en los países desarrollados se está desacelerando y desacoplando a la demanda. El consumo de energía eléctrica en Estados Unidos y la Unión Europea es del 40% mundial, mientras que en otros países sobre todo economías emergentes sigue creciendo [48]. No sólo se trata de generar más electricidad sino de generarla de forma más eficiente y menos contaminante, a este proceso se le ha denominado como descarbonización.

En los últimos años, se han sumado nuevos cambios tecnológicos y tendencias a la REI como lo son el incremento del uso de Vehículos Eléctricos (VE) lo que ha traido consigo el concepto de movilidad eléctrica, el uso de sistemas de almacenamiento de energía y particularmente la generación de electricidad a través de energías renovables como la solar y eólica haciendo uso de paneles fotovoltaicos y aerogeneradores. A esto último se le ha denominado microgeneración por parte de los consumidores finales, lo que los ha convertido en pequeños productores de electricidad. Debido al abaratamiento de las fuentes de energía distribuida renovable, el rol de los usuarios finales ha cambiado a ser prosumidores (productores-consumidores) en donde los usuarios finales pueden generar su propia energía eléctrica y debido a la gran intermitencia de las energías limpias también pueden consumir

energía de la empresa eléctrica. A su vez, el excedente de energía eléctrica puede ser comercializado a otros consumidores, a las empresas suministradoras y a otros participantes del mercado eléctrico a través del concepto de energía transactiva. Todos estos cambios se ilustran en la **Figura 2-1**.

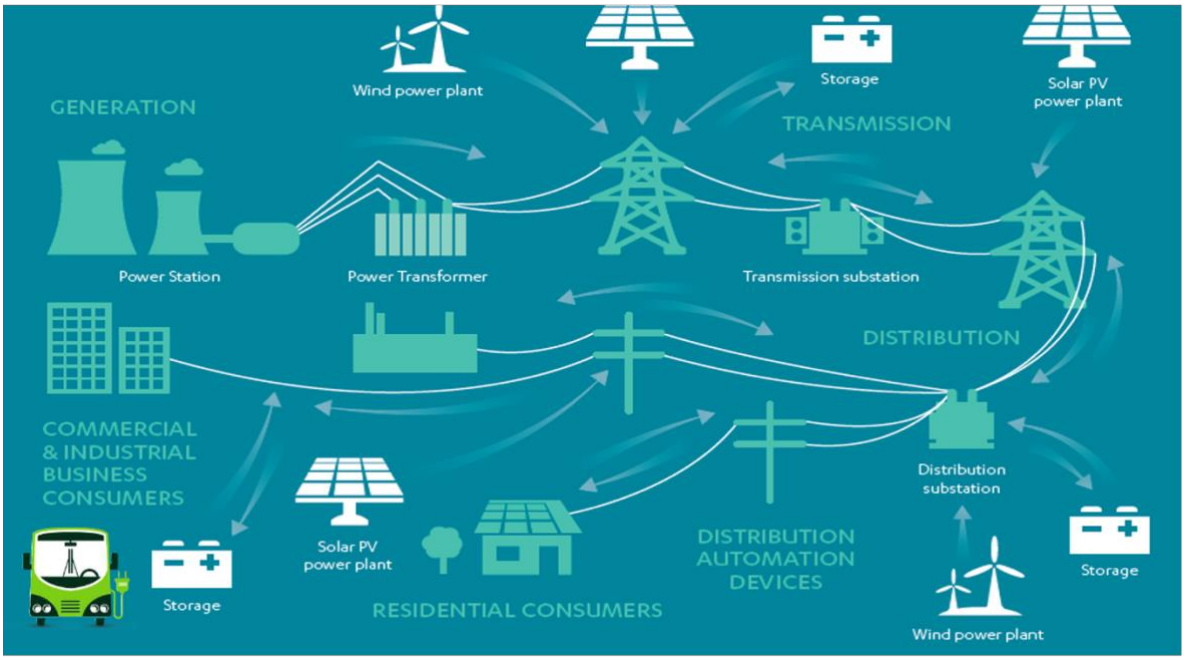

Figura 2-1 *Nuevas Tecnologías en la REI [49].*

La REI es uno de los pilares fundamentales de las Ciudades Inteligentes (ver

Figura **2-2**), en donde la tecnología se conjunta con el medio ambiente para tomar decisiones sostenibles a largo plazo.

La REI ha evolucionado en los últimos años, pero debe su gran auge a la invención de los medidores eléctricos inteligentes. Un medidor inteligente (MI) permite la medición del consumo y/o producción de energía eléctrica y reportarlo a través de redes de telecomunicaciones a la empresa eléctrica, facilitando el proceso de lectura de las mediciones y su rápida facturación [48]. Además de estos beneficios también se cuentan otros como cortes y reconexiones de forma automática, reportes periódicos de consumo de energía, interconexión con sistemas de gestión de energía y de respuesta a la demanda [51].

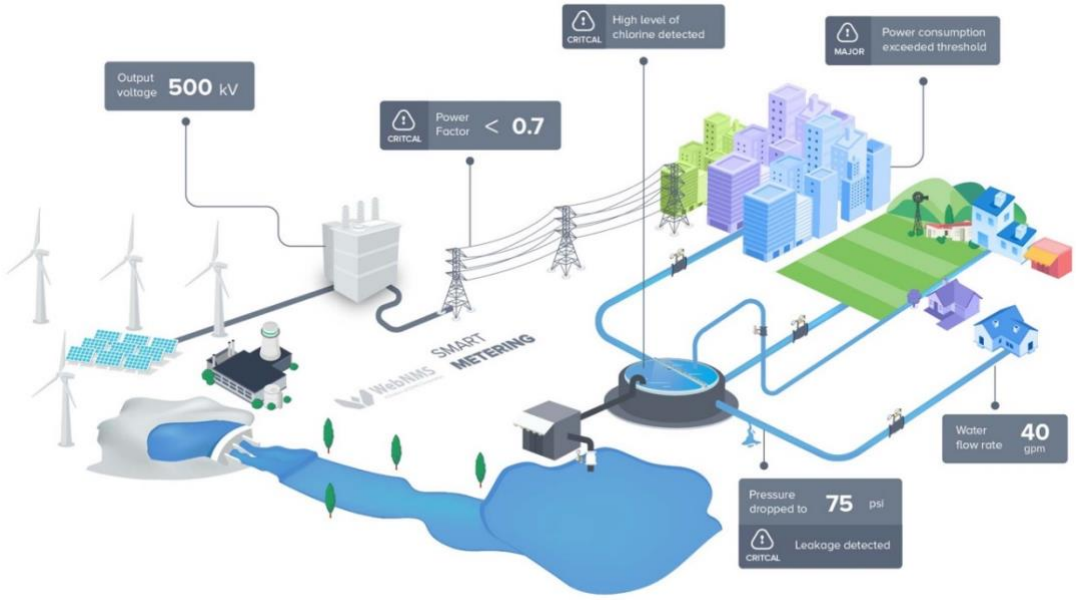

Figura 2-2 *Ciudades inteligentes [50].*

En la Figura **2-3** se muestran las principales tareas que realiza un MI. Los MI son sistemas embebidos con capacidades de comunicación (hoy en día conocidos como de IoT) que cuentan con capacidades de procesamiento y almacenamiento de información limitadas si se compara con equipos de cómputo personal, pero que hoy en día pueden ejecutar un sinfín de aplicaciones a través de interfaces de usuario.

El MI no sólo es capaz de medir en tiempo real el consumo eléctrico, sino que también puede medir otras variables de la señal eléctrica como: voltaje, ángulo de fase, factor de potencia, frecuencia, entre otras [52]. Además, el MI debe comunicar de manera segura estos datos tanto al usuario, como al proveedor de la energía, centros de procesamiento de datos o cualquier organismo habilitado para la recolección y procesamiento, tales como entes reguladores [53]. Por este motivo los MI son buenas opciones para el control de la calidad de la energía y la detección de fallas.

Entre las nuevas aplicaciones de los MI se encuentran la capacidad de hacer análisis en tiempo real de los datos, lo que permite, a través de algoritmos de analítica de datos, identificar aquellos registros que distan considerablemente del consumo habitual, sin embargo, el cambio en la tendencia y/o patrón del consumo no necesariamente implica una causal de actos ilícitos o errores de medición, existen muchas variables que pueden modificar la cantidad de energía eléctrica que un usuario puede consumir por periodo de tiempo, desde

variables climatológicas hasta gustos y preferencias en electrodomésticos, dispositivos; nivel adquisitivo, cohabitantes, etc. [54].

Figura 2-3 *Principales tareas de un medidor inteligente.*

A pesar de todas las ventajas que presentan los MI, también presentan algunas desventajas; por ejemplo, bajo el esquema tradicional de facturación de energía eléctrica, la energía eléctrica tiene que ser consumida donde se necesita por lo que los usuarios finales no podrían cargar sus vehículos eléctricos o cualquier otra carga eléctrica de alto consumo en distintos puntos (por ejemplo, la casa de un familiar) si ésta no se factura al usuario correcto (esto debido al alto consumo de energía eléctrica que lo hace costoso). Para lograr la movilidad eléctrica, se deben resolver nuevos desafíos, como la medición inteligente del consumo de energía y sobre todo la ciberseguridad de estas mediciones.

Para poder lograr estas prestaciones se requiere, además de los medidores inteligentes, de otros componentes e infraestructura tecnológica, siendo la más extendida la AMI [55]. AMI permite recolectar datos en diversos niveles a través de los concentradores de datos además

de poseer un centro de datos en la empresa eléctrica para poder trabajar con el amplio volumen de información generada por los medidores inteligentes [56].

De manera general, los SMI se conceptualizan con cuatro elementos básicos: en primera instancia los medidores inteligentes y otros equipos de medición como los Concentradores de Datos (CD), una red de telecomunicaciones tanto de forma cableada como inalámbrica robusta, un centro de datos donde se almacena y procesa toda la información, y finalmente, las aplicaciones que explotan los datos, esto se ilustra en la Figura **2-4**.

Los sistemas de medición inteligente incluyen diversos componentes, los cuales se muestran de manera completa en la Figura **2-5** y de manera general en la Figura **2-6** (generalmente los componentes de telecomunicaciones se omiten).

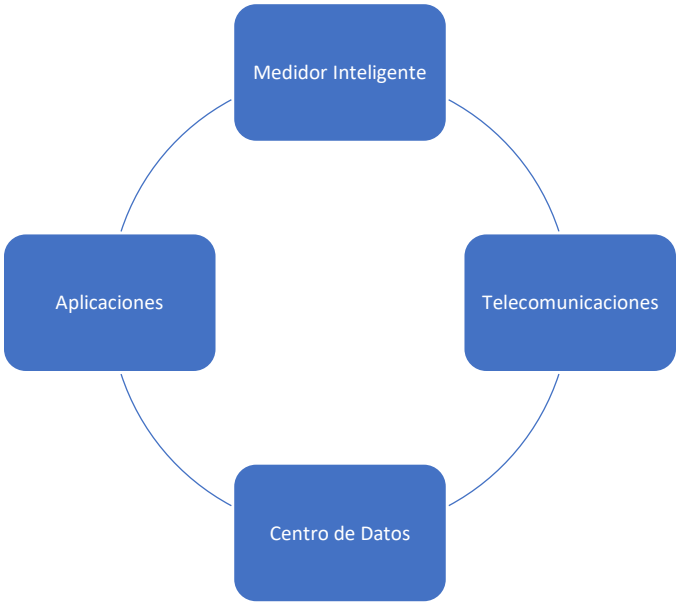

Figura 2-4 *Sistemas de Medición Inteligente.*

Los MI no sólo miden el consumo de energía de los electrodomésticos (E) y los electrodomésticos inteligentes (EI). A su vez, regulan la producción de energía de los Recursos Energéticos Distribuidos (DER). Estos dispositivos se conectan en una pequeña red de telecomunicaciones de área local denominada Red de Área Hogareña (HAN por sus siglas en inglés) si el consumo es en el hogar, ya que si está en un edificio se llama Red de Área de Edificios (BAN por sus siglas en inglés). Si el consumo se realiza en la industria, se denomina Red de Área Industrial (IAN, por sus siglas en inglés).

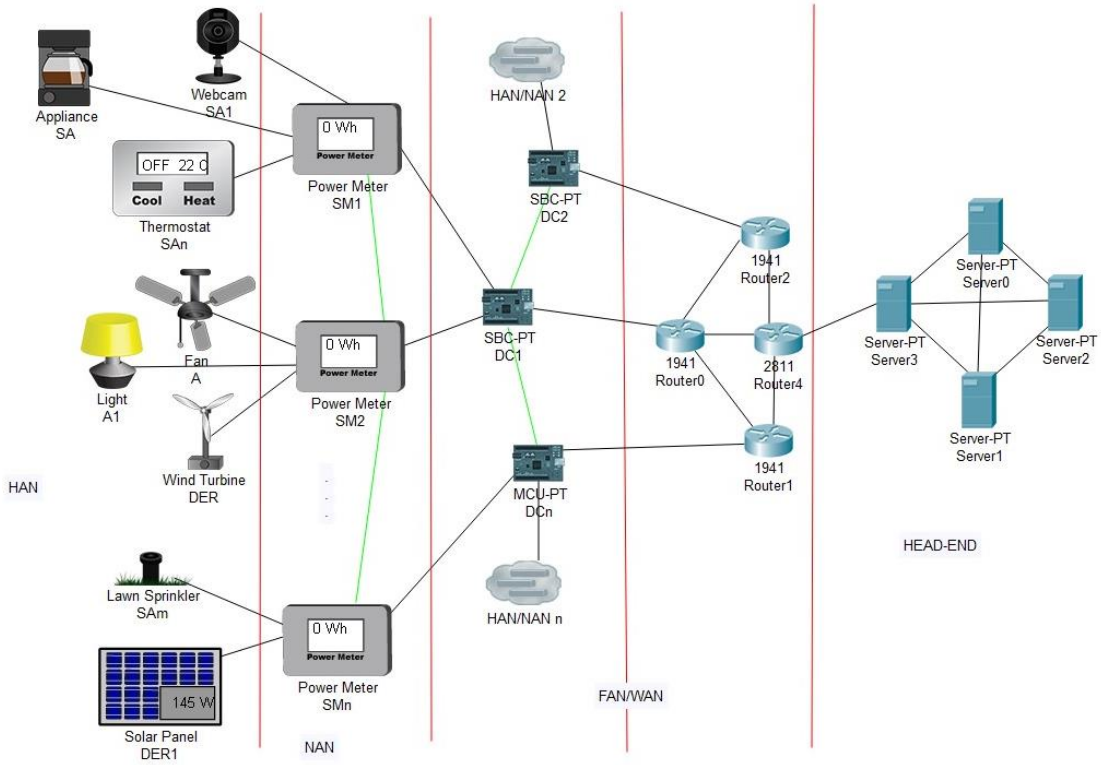

Figura 2-5 *Arquitectura completa de un SMI.*

Los MI se conectan a otros medidores o directamente a CD mediante una red de datos llamada Red de Área de Vecindario (NAN, por sus siglas en inglés). Los CD son los encargados de concentrar la información de los distintos medidores en las redes de distribución. Dependiendo de su ubicación geográfica y su alta densidad de nodos (MI y CD), los CD pueden comunicarse entre sí mediante una red de área amplia (WAN, por sus siglas en inglés), que, debido a las duras consideraciones de alto voltaje y clima, se denomina red de área de campo (FAN, por sus siglas en inglés). Finalmente, los datos de los CD llegan al centro de datos de la empresa de servicios públicos llamada Head-End. En el centro de datos, los datos se almacenan en grandes grupos de computadoras y se interconectan con otros sistemas de la empresa de servicios públicos.

Tradicionalmente, los datos se almacenan en BD en los CD y los servidores de bases de datos de las empresas de servicios públicos. Recientemente, los MI de nueva generación comienzan a tener mayores capacidades de almacenamiento y procesamiento que les permiten nuevas aplicaciones derivadas de la analítica de datos.

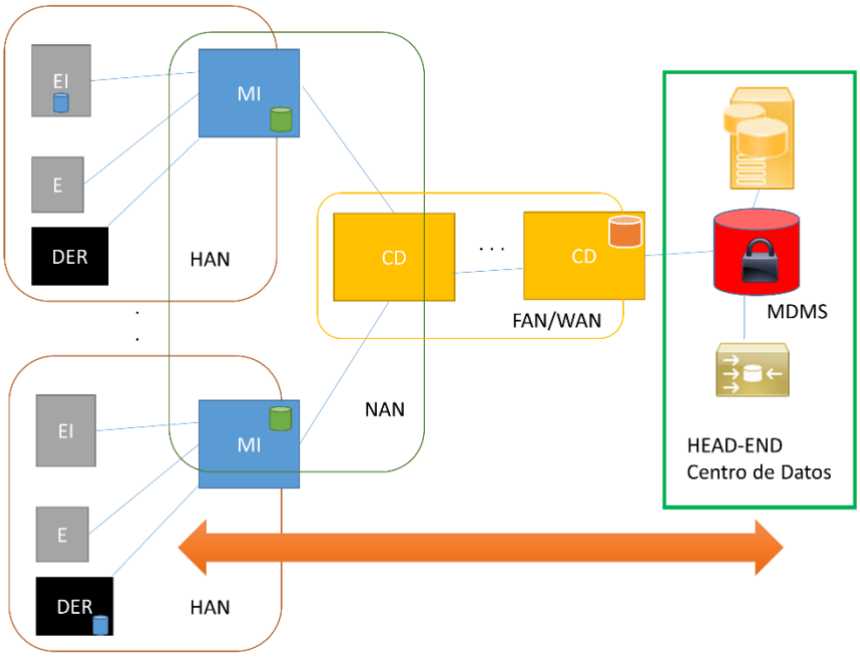

Figura 2-6 *Arquitectura general de un SMI.*

El Sistema de Gestión de Datos del Medidor (MDMS, por sus siglas en inglés) es un componente esencial en el funcionamiento de un sistema de medición inteligente [57]. Es una plataforma de software que recolecta datos de diferentes tecnologías de contadores inteligentes, verifica y almacena la información para luego ser entregada en subconjuntos a las distintas aplicaciones comerciales como facturación, gestión de apagones, etc.

Los medidores inteligentes registran eventos, cargan perfiles, precios y transmiten datos a usuarios y proveedores. Los consumidores pueden comprobar su uso de la electricidad y controlar su consumo. Los concentradores suelen estar ubicados en las subestaciones y recopilan los datos de los medidores. Se conecta un promedio de 500 MI a los CD.

2.1.1. Sistemas Ciberfísicos en SMI

Los sistemas ciberfísicos están compuestos por 4 elementos fundamentales: objetos, personas, procesos y datos; como se puede ver en Figura **2-7**.

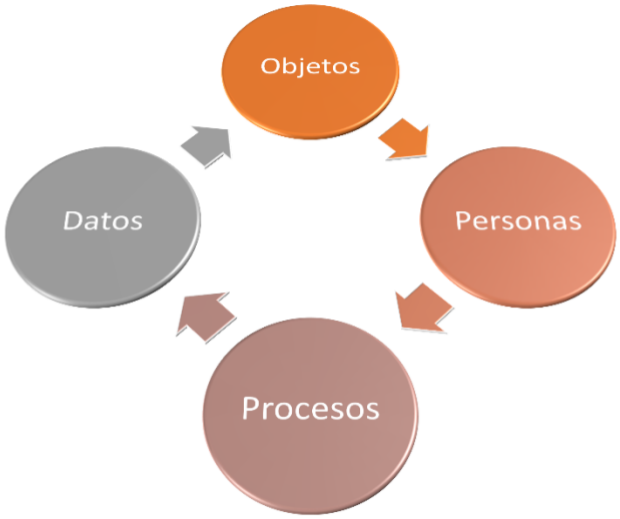

Figura 2-7 *Elementos principales de un sistema ciberfísico.*

Particularmente los SMI se pueden adaptar a este modelo tal y como se muestra en la Figura **2-8**. Las personas son la capa más importante ya que son los usuarios y operadores del sistema. La persona principal es el prosumidor que consume y produce energía eléctrica, es quien realmente utiliza el sistema, es el cliente final. Por otra parte, se ocupa personal especialista en SEP y del área de TICs. Los objetos hacen referencia a los diversos elementos físicos del sistema (hardware) como lo son los MI, electrodomésticos, dispositivos electrónicos, CD, sistemas de información de la empresa eléctrica, aplicaciones (software), entre otros. Tanto los objetos como las personas generan datos, los cuales se almacenan dependiendo de las capacidades de los objetos y se acceden dependiendo de los roles que tengan las personas. Finalmente, los procesos se implementan dentro del software o bien los ejecutan las personas y son las actividades que en conjunto se realizan dentro del sistema ciberfísico.

2.1.2. Arquitecturas de Cómputo Distribuido en REI y SMI

En el pasado, los equipos de cómputo eran 100% centralizados en grandes computadoras denomindas mainframes. Con el avance en la minutarización de componentes eléctronicos y su abaramiento empezaron a surgir esquemas de cómputo cada vez más descentralizado como la arquitectura cliente servidor que es la base de funcionamiento de las aplicaciones de Internet. Esto ha derivado en la evolución del concepto que se ha denominado computación en la nube, en donde una gran cantidad de servidores e infraestructura tecnológica se conjunta de forma transparente para el usuario final y en la que se proporciona hoy en día una gran cantidad de servicios [58].

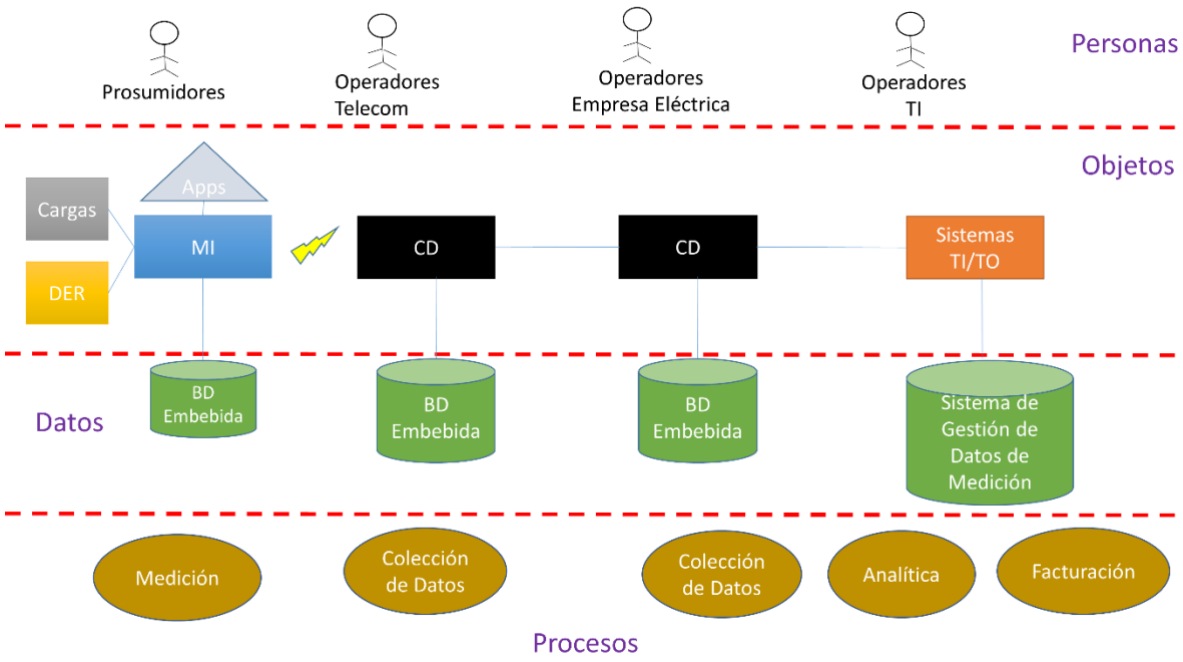

Figura 2-8 *Modelo ciberfísico de los SMI.*

Desafortunadamente el cómputo en la nube es un esquema que, si bien es distribuido, por que se manejan una gran cantidad de servidores de manera conjunta para brindar los servicios proporcionados, es jerarquicamente centralizado. Desde hace tiempo se han tratado de ejecutar procesos más pesados en el lado del cliente, hoy en día esto es posible con los procesos de par a par (P2P, por sus siglas en inglés) en los que se trabaja de forma igualiataria diviendo el trabajo.

Recientemente, con el auge de los dispositivos IoT, se ha tratado que estos dispositivos realicen procesos más que el simple sensado del medio o el cerrado de circuitos. A esta tendencia se le ha denominado computación en el borde (*edge computing*) y es cada vez más utilizada debido al incremento de capacidades de procesamiento y almacenamiento de los dispositivos IoT [59].

Por otra parte, en algunos contextos, entre la computación en la nube y en el borde existe un inmenso espacio que hasta hace poco no había sido explorado y a lo que se ha denominado cómputo en la niebla. El cómputo en la niebla permite tener pequeñas nubes más cercanas a donde se generan los datos siendo mucho más fáciles de procesar consultas que no necesitan los datos globales, teniendo una respuesta mucho más rápida para los clientes finales pero sobre todo hacer del cómputo en la nube más escalable y modular [22].

En la Figura ***2-9*** se muestra un esquema general de la arquitectura distribuida borde-niebla-nube, donde la capa de borde está representada por dispositivos de baja capacidad de procesamiento de datos pero conectados a los sensores y actuadores que es en donde se originan los datos. La capa de niebla tradicionalmente son servidores que concentran la información de varios dispositivos en el borde, típicamente pueden están colocados dentro de los diferentes nodos intermedios de comunicación de las empresas. Finalmente, se encuentra la capa de nube en donde se concentra toda la información y se realiza todo el procesamiento global.

La arquitectura de cómputo distribuido borde-niebla-nube ha empezado a ser ampliamente utilizada dentro de los sistemas ciberfísicos ya que se puede ajusta a muchos problemas de forma simple y para el caso de la REI no es la excepción.

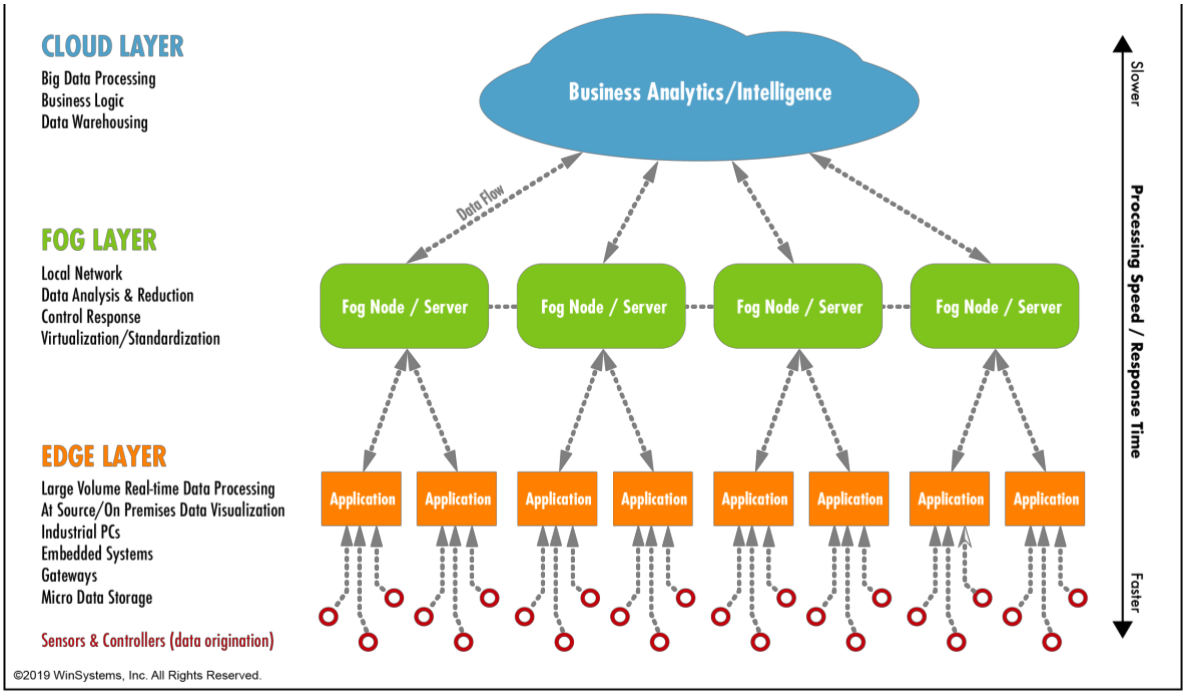

Figura 2-9 *Arquitectura de cómputo distribuida nube-niebla-borde [60].*

2.1.3. Radiación Electromagnética de MI

Hoy en día, existe una gran preocupación por el hecho de que los datos de los MI, que se comunican principalmente por medios de comunicación inalámbricos o por cable, puedan producir campos electromagnéticos que sean perjudiciales para la salud humana.

Los Campos ElectroMagnéticos (CEM) se caracterizan principalmente en términos de frecuencia e intensidad. La frecuencia está relacionada con la cantidad de ondas que pasan

por un lugar fijo en un período de tiempo determinado. Se mide en hercios (Hz), que expresa el número de ondas por segundo. Normalmente, las señales EM se dividen en dos categorías, no ionizantes e ionizantes [61]. La radiación CEM ionizante es dañina para los seres vivos. Sin embargo, los campos electromagnéticos no ionizantes podrían ser peligrosos para los seres humanos si la densidad, el tiempo y la fuerza de las señales son altos. Las intensidades de la señal (densidad de potencia) se miden en diferentes unidades, según la frecuencia y la naturaleza de la señal: Gauss (G), Voltios (V), Watts (W), entre otros [62].

Los MI funcionan con tarjetas de interfaz de red (NIC) inalámbrica en un espectro de radiofrecuencia (RF) entre 900 MHz y 2,45 GHz. No existen unidades estándar para medir la radiación de RF, pero las más comunes son: ($\mu W/m^2$), ($\mu W/cm^2$) y (V/m). Los dispositivos electrónicos, como teléfonos móviles, hornos microondas, refrigeradores y MI inalámbricos producen emisiones de RF. Por otro lado, los dispositivos de IoT y otros dispositivos electrónicos han aumentado la contaminación por RF.

La exposición a emisiones de RF puede provocar efectos térmicos y no térmicos. Los efectos térmicos en los seres humanos se han estudiado ampliamente y parecen entenderse bien. La Comisión Federal de Comunicaciones (FCC, por sus siglas en inglés) ha establecido pautas para proteger la salud pública de los peligros conocidos asociados con los impactos térmicos de la RF: el calentamiento de los tejidos por absorber la energía asociada con las emisiones de RF [63]. Las ondas electromagnéticas transportan energía y los CEM absorbidos por el cuerpo pueden aumentar la temperatura del tejido humano. El consenso científico es que la temperatura corporal debe aumentar al menos 1 °C para provocar posibles impactos biológicos del calor [64]. Sin embargo, los efectos no térmicos, incluida la exposición acumulada o prolongada a niveles más bajos de emisiones de RF, no se comprenden bien. Algunos estudios han sugerido que los efectos no térmicos pueden incluir fatiga, dolor de cabeza, irritabilidad o incluso cáncer [63].

Los ciclos de trabajo actuales del transmisor del MI (es decir, el porcentaje del tiempo que opera el medidor) serían típicamente del 1%, o en algunos casos donde el medidor se usa con frecuencia como relé, puede ser entre el 2 y 4% [61]. Esto significa que SM no transmite datos con mucha frecuencia (en AMI, el tiempo típico para el informe de datos es de 15 minutos), pero en el futuro, si se agregan nuevas aplicaciones y funcionalidades a los MI, el período de transmisión de datos podría aumentar los ciclos de trabajo del MI. Por ejemplo, si los eventos de calidad de la energía se informan en tiempo real, los ciclos de trabajo en SM podrían alcanzarse al 100% como en una transmisión de TV o radio FM.

La Tabla **2-1** muestra el tiempo promedio de exposición de algunos dispositivos electrónicos. Además, los MI se pueden utilizar con otros servicios públicos como agua y gas. Esto podría incrementar la exposición a RF de los seres humanos en los próximos años.

Tabla 2-1 *Tiempo de Exposición.*

Dispositivo	Densidad Máxima	Tiempo (s)
MI	1%	0.1
Horno	25%	15
Celular	5%	1000
Luces	7%	10,000
Cables de Transimisión y Distribución	0.05%	>10,000

Los problemas de salud que rodean la RF de los MI son similares a los de muchos otros dispositivos que usamos en nuestra vida diaria, incluidos teléfonos inalámbricos y móviles, hornos microondas, enrutadores inalámbricos, secadores de pelo y computadoras portátiles con capacidad inalámbrica [65]. Los problemas de salud podrían aumentar si los MI se encuentran en un edificio multifamiliar como un edificio de apartamentos debido a que hay varios MI juntos en la misma ubicación, pero para ello son necesarios alrededor de 100 MI o más además de permanecer en las instalaciones eléctricas durante más de 30 minutos. La Tabla **2-2** muestra los diferentes niveles de RF en los dispositivos electrónicos comunes que incluyen MI [65]. Como puede observarse, no existen trabajos concluyentes de que los MI sean malos para la salud.

2.2. Ciberseguridad en REI y SMI

La ciberseguridad es hoy en día una de las principales preocupaciones en el área de las TICs. Dada la gran penetración de TICs en diversas áreas del quehacer humano entre ellos los SEP, la protección de la infraestuctura eléctrica tanto de flujo de energía y de tecnología se ha vuelto de suma importancia, ya que al final de cuentas se traduce en pérdida de dinero.

Los ataques cibernéticos se han vuelto cada vez más frecuentes en las infraestructuras críticas particularmente en la REI. A continuación, se mencionan brevemente algunos estadísticos que demuestran el incremento en ciberataques en la REI.

Tabla 2-2 *Niveles máximos de RF en algunos dispositivos.*

Fuente	Frecuencia	Nivel de Exposición ($\mu W/cm^2$)	Distancia	Tiempo	Caracteristica Espacial
Celular	900 MHz, 1800 MHz	1 - 5	En el oído	Durante una llamada	Altamente localizable
Horno de microondas	2.45 GHz	50.05 – 0.2	5 cm, 60 cm	Durante el uso	Localizado, no uniforme
WLAN	2.4 – 5 GHz	0.001, 0.0002	1 m	Constante cuando está cerca	Localizado, no uniforme
Transmisión Radio/TV	Wide spectrum	0.001	Lejos de la fuente	Constante	Relativemente uniforme
MI	900 MHz, 2400 MHz	0.001 (250 mW, 1% ciclo de trabajo) 0.002 (1 W, 5% ciclo de trabajo)	3 metros	Cuando se está en proximidad durante la transmisión	Localizado, no uniforme

El Equipo de Respuestas ante Emergencias Cibernéticas – Sistemas de Control Industrial (ICS-CERT, por sus siglas en inglés) de Estados Unidos señala que cerca de 32% de los ataques industriales fueron al sector energético [66]. Por otra parte, se estima que el 55% de los incidentes investigados en 2020 mostraron señales de Amenazas Persistentes Avanzadas (APT, por sus siglas en inglés). La empresa de servicios públicos Lansing Board of Water & Light pagó $25,000 dólares estadounidenses a través de un ataque de Ransomware en 2017.

La ciberseguridad consiste en la protección de los activos de información de una organización u objeto de estudio dado. Particularmente, las premisas básicas de la ciberseguridad son conocidas como CIA (por sus siglas en inglés de Confidentiality, Integrity and Availability), las cuales hacen referencia a la Confidencialidad, Integridad y Disponibilidad de la Información. Adicionalmente en entornos industriales y de misión crítica como lo es la REI se ha agregado una cuarta premisa que es la Seguridad Física, ya que la seguridad de las personas es lo más importantes y en algunas partes de la REI la ausencia de ciberseguridad

puede ocasionar la muerte. Por lo que el concepto de CIA evoluciona a CIAS para incluir la parte de seguridad física.

En la Figura **2-10** se muestran las premisas básicas de la ciberseguridad, mientras que en la Ecuación 1 se muestra la fórmula general empírica de la ciberseguridad. La ciberseguridad está expresada como un riesgo de que un incidente malicioso pueda ocurrir. El riesgo se puede medir como una probabilidad de ocurrencia de dichos incidentes maliciosos y como tal se mide de 0 a 100%. La ciberseguridad está dada por factores externos conocidos como amenazas (típicamente los ciberataques), los cuales se aprovechan de las vulnerabilidades de los sistemas (factores internos, considerados como huecos de seguridad). El riesgo puede ser mitigado; es decir, reducido más no eliminado a través de contramedidas o controles, los cuales ayudan a subsanar (parchar) las vulnerabilidades de los sistemas para lograr mayor protección. Dado que la tecnología siempre avanza, los retos de ciberseguridad siempre estarán presentes, por lo que se hace necesario contar con Sistemas de Gestión de Seguridad Informática (SGSI) que ayuden a planear, controlar, verificar y actuar ante la presencia de riesgos informáticos.

Figura 2-10 *Premisas básicas de ciberseguridad.*

$$Riesgo = \frac{Amenaza * Vulnerabilidad}{Contramedidas}$$

Ecuación 1 *Fórmula empírica del riesgo*

La ciberseguridad es la combinación de diversas tecnologías, procesos y controles diseñados para eliminar los riesgos de ciberataques [67]. Las consecuencias de una violación de la seguridad son diversas. Los efectos significativos son reputación arruinada, vandalismo, robo, pérdida de ingresos, daños a la propiedad intelectual, entre otros. El uso de dispositivos IoT, sistemas integrados y otros sistemas físicos cibernéticos ha aumentado el riesgo de ataques cibernéticos [68].

La ciberseguridad de cualquier sistema viene dada por la ciberseguridad del mínimo elemento de su arquitectura; en este caso, todos los objetos de la REI tanto físicos como virtuales, incluidos los humanos [69].

La ciberseguridad y la privacidad de los datos en los SMI es esencial. Es importante que se protejan las lecturas tanto del consumo como de la producción de energía eléctrica. A su vez, es necesario que dicha información, si es compartida, cuente con el consentimiento informado del cliente, ya que esta información se clasifica como datos personales.

Por otra parte, los piratas informáticos (*hackers*) pueden robar, manipular e interrumpir los SMI. Existe la posibilidad de afectar a escalas diferentes la REI mediante el ataque a los sistemas de Supervisión, Control, y Adquisición de Datos (SCADA, por sus siglas en inglés) y los MI. La REI es una red distribuida, administrada centralmente, de millones de dispositivos listos para ser atacados. Tradicionalmente, la ciberseguridad en la REI se ha centrado en los sistemas SCADA porque la protección de los activos más importantes es vital debido a la descentralización de la REI [70]. Los sistemas SCADA están presentes en los procesos de generación, transmisión y distribución en las empresas de servicios públicos.

La Tabla **2-3** muestra tres ejemplos de riesgo en la REI, mientras que la Tabla **2-4** muestra los impactos y la estimación de estos riesgos. La estimación del riesgo se debe realizar con base en una metodología previa establecida ya sea que esté basada en una recomendación o norma, o bien por cuenta propia.

Las amenazas externas pueden ser personas ajenas como ciberdelincuentes, piratas informáticos, hacktivistas, terroristas y fanáticos. Las amenazas internas pueden ser empleados y ex empleados, subcontratación de personal y socios confiables.

Otras amenazas son errores humanos, fallas de hardware, sabotajes y errores de software, entre otros. Por el contrario, algunos ejemplos de vulnerabilidades son desbordamiento de búfer, entradas no validadas, condiciones de carrera, debilidades en las prácticas de seguridad, problemas de control de acceso, entre otros.

Tabla 2-3 *Ejemplo de riesgos en la REI.*

Riesgo	Amenaza	Vulnerabilidad
Apagones	Conmutación de prendido/apagado de forma remota.	Mala configuración de red que permite acceder a una terminal remota.
Sistema Comprometido	Clonación del MI.	Reporte de alarma débil cuando un MI es cambiado.
Secuestro o Robo del MI o CD	Actualización Remota	Privilegioss incorrectos para usuarios remotos.

Tabla 2-4 *Ejemplos de impacto de riesgos en la REI.*

Riesgos	Impacto	Estimación
Apagones	Desconexión de una casa, edificio o industria.	Baja
Sistema Comprometido	Las lecturas del cliente de consumo/producción no son correctas y no pueden ser facturadas adecuadamente.	Alta
Secuestro o Robo del MI o CD	El MI es secuestrado y no está disponible para la empresa eléctrica.	Media

Una vulnerabilidad puede ser producida por malware como *spyware, adware, bot, ransomware, scareware, rootkit*, virus, troyanos, gusanos, Hombre en el Medio (MitM, por sus siglas en inglés) y Hombre en el Móvil (MitMo, por sus siglas en inglés). Algunos ciberintrusos podrían descifrar contraseñas WiFi a través de algunos ciberataques, como ingeniería social, ataques de fuerza bruta y monitoreo de red.

En la mayoría de los casos, las contramedidas y los controles de ciberseguridad dependen de las políticas de ciberseguridad. Las políticas están relacionadas sobre cómo se podrían proteger los activos para garantizar la seguridad cibernética. La implementación de estas

políticas implica el uso de mejores prácticas y contramedidas. La Tabla **2-5** muestra algunos ejemplos de políticas de ciberseguridad y contramedidas para implementarla en SG.

Tabla 2-5 *Ejemplo de políticas de ciberseguridad en REI.*

Políticas	**Contramedidas / Mejores Prácticas**
Analizar todas las entradas y salidas de paquetes de red	Mantener un cortafuegos
Usar un antivirus y antispyware	Tener actualizado los sistemas
Uso de contraseñas únicas para cada cuenta en línea	Usar un software llavero para almacenar y recuperar contraseñas
Usar contraseñas robustas (no usar palabras de diccionario o nombres en cualquier lenguaje, si es possible, usar caracteres especiales tales como ¡@ # $% & * (), y usar contraseñas con diez o más caracteres)	Implementar contabilidad de contraseñas cuando una nueva contraseña sea creada
Acceso remoto restringido a cuentas privilegiadas	Configurar acceso remoto a software que no permita cuentas de root o admin conectadas directamente a los servicios.

Con respecto a las amenazas físicas, restringir el acceso al hardware MI es extremadamente importante. El hardware puede manipularse por exposición a perturbaciones externas, como imanes permanentes, que inducen errores en las lecturas de consumo. Otra amenaza física consiste en cambiar los componentes electrónicos de MI por otros componentes dañados. En algunos casos, el MI se reemplaza con un MI alterado. Por esta razón, los MI suelen estar encapsulados para que sus componentes no sean manipulados para robar energía [71].

Uno de los ataques de red de comunicación de datos más comunes en SMI consiste en inyectar paquetes de datos falsos en las redes de comunicación, donde los precios en tiempo real generalmente se ven afectados [72], [73] y [74]. En general, la manipulación a través de ataques de datos incorrectos da como resultado lecturas de consumo / producción alteradas,

eventos de desconexión y reconexión, entre otros. Otros ataques similares son la retransmisión de paquetes para generar Denegación de Servicio (DoS, por sus siglas en inglés). Con respecto a la seguridad de los CD y otros IED, las preocupaciones de seguridad son muy similares a las de MI. La seguridad en los centros de datos es muy importante, particularmente en los MDMS, que es la infraestructura de servicios informáticos donde se almacena toda la información de las lecturas MI.

El principal mecanismo de ciberseguridad implementado hoy en día radica en el uso de técnicas criptográficas. La criptografía permite que los datos se cifren, almacenen y transmitan de forma segura. Solo las personas con acceso adecuado pueden descifrar esta información.

La criptografía basa su funcionamiento en funciones y algoritmos matemáticos que requieren una alta potencia computacional, lo que la convierte en un desafío en dispositivos IoT y en REI no es la excepción. Para ello, muchos trabajos se han centrado en algoritmos y funciones criptográficas ligeras que pueden funcionar correctamente en REI, particularmente en SMI que a pesar de ser ligeros son robustos por lo que no son fácilmente descifrables [75].

Dentro de las diversas técnicas criptográficas, las funciones hash han destacado en las últimas fechas. Las funciones hash son funciones criptográficas que, dada una entrada, producen una única salida. Esta salida tiene un tamaño predeterminado que está determinado por la función hash y no es reversible; es decir, a través de la salida, no puede obtener la entrada. Las funciones hash sirven para validar la integridad y consistencia de los datos, por lo que hoy en día son los mecanismos más utilizados en la actualidad para validar la integridad de los datos por su sencillez de uso y fácil adaptación a dispositivos IoT y SMI.

El principal problema de la criptografía es el intercambio de las claves que permiten descifrar los mensajes. La criptografía generalmente por su forma de manejar las claves se ha dividido en simétrica y asimétrica.

En criptografía simétrica con una sola clave, el mensaje se cifra y se descifra. El problema radica en compartir esta clave porque preferiblemente debe hacerse a través de un canal seguro. Para evitar esto, surgió la criptografía asimétrica para evitar este tipo de problemas. Por lo tanto, generalmente se usan dos claves: una clave pública y una clave privada. Cuando el remitente desea enviar un mensaje, es necesario conocer la clave pública del destinatario. Estas claves públicas se pueden compartir sin ningún problema. Sin embargo, las claves privadas deben guardarse rigurosamente. Conociendo la clave pública del destinatario, el remitente con su clave pública y privada cifra el mensaje enviado al destinatario. El receptor para descifrar el mensaje ocupa la clave pública del emisor para verificar que fue enviado por esta persona y junto con su clave pública y privada puede descifrar el mensaje.

Debido a sus grandes ventajas, la criptografía de clave asimétrica se ha utilizado ampliamente en esquemas de seguridad como las firmas digitales. Para ello, debe contar con Autoridades de Certificación (CA, por sus siglas en inglés) que le permitan conservar los certificados de identidad de cada una de las partes. Con esto surge el problema de la administración de certificados y claves públicas. Se han ideado varios mecanismos para solucionarlo, siendo la Infraestructura de Clave Pública (PKI, por sus siglas en inglés) la más popular.

El problema con PKI y otros mecanismos de intercambio de claves públicas es que a medida que los participantes crecen, su funcionamiento se vuelve más complejo y, en general, es un mecanismo centralizado. Por estos motivos, se ha convertido en un problema para los dispositivos IoT y SMI, por lo que en la actualidad muchos trabajos de investigación se han centrado en solucionar esta parte. Otros trabajos se han centrado en mecanismos más eficientes y seguros en firmas digitales, IPS, IDS, entre otros [76].

En la actualidad, los IDS son uno de los enfoques de seguridad más utilizados. Los IDS son sistemas que permiten detectar intrusos en cualquier tipo de sistema. Por lo tanto, los IDS utilizan mecanismos para predecir comportamientos anómalos basados en patrones de comportamiento previamente definidos. Los IDS son complicados de implementar de manera eficiente en dispositivos con recursos limitados, como en dispositivos IoT y SMI, debido al alto consumo de recursos computacionales. Además, los IDS basan su funcionamiento en estadísticas de uso y posibles malos comportamientos. Por lo tanto, el IDS puede ser probabilístico en muchos casos y puede no detectar intrusos que se aparten de los patrones preestablecidos. Para ser más eficientes en las predicciones IDS, los trabajos de investigación se han centrado en desarrollar mecanismos IDS más ligeros que permitan una detección más precisa de intrusos [77].

La seguridad de las telecomunicaciones es otro aspecto relevante de los SMI. Los datos medidos por el SM se informan a la empresa de servicios públicos a través de su red de datos. Por lo general, parte de la red se alquila a un Proveedor de Servicios de Internet (ISP, por sus siglas en inglés). Por otro lado, la mayor parte de la conectividad de los dispositivos IoT y SMI es por medios inalámbricos, lo que facilita la conectividad, pero habilita otras vulnerabilidades de ciberseguridad. Por ejemplo, si los datos son interceptados por el ataque MitM, los datos pueden modificarse y generar grandes pérdidas económicas para la empresa de servicios públicos. Los trabajos de investigación se han centrado en fortalecer la pila de protocolos de comunicación con esquemas más seguros utilizando mecanismos como la criptografía y la autenticación, además de agregar servicios de red más seguros como Red Privada Virtual (VPN, por sus siglas en inglés), Secure Shell (SSH, por sus siglas en inglés), Protocolo Seguro de Transferencia de Archivos (SFTP, por sus siglas en inglés), entre otros [78].

Con respecto a la seguridad del software, los MI están comenzando a manejar arquitecturas basadas en computadoras de placa única (SBC, por sus siglas en inglés) como, por ejemplo, Raspberry Pi, que aumentan significativamente las capacidades computacionales de MI debido a los sistemas operativos (SO) inherentes utilizados, como Linux embebido. A pesar de la mayor potencia computacional disponible, existen otras posibles brechas de seguridad, ya que será necesario fortalecer la seguridad de las aplicaciones SMI y servicios adicionales (por ejemplo, bases de datos integradas y servidores web) así como el propio SO [58].

En la actualidad, hay trabajos enfocados a lograr la ciberseguridad para REI. Aún así, faltan trabajos centrados en la ciberseguridad, que considera al factor humano como un elemento vital para proteger los activos de la REI.

Recientemente, ha surgido el concepto de Ciber Higiene que, aunque no existe una definición única [79], pero la mayoría de los autores la consideran una analogía con la higiene diaria. Por ejemplo, la idea de lavarse las manos y los dientes podría mejorar la salud personal. Por ejemplo, así como en salud pública la higiene personal de cada persona contribuye a la salud global de la población, también se requiere la participación de otros actores como el gobierno dado que la comunidad necesita algunos servicios públicos como limpieza de calles, recolección de basura, entre otros. Estos servicios públicos son necesarios para la asistencia sanitaria. En ese mismo contexto, el suministro de energía eléctrica es un servicio público proporcionado por las empresas de servicios públicos, por lo que la ciberseguridad de la REI resulta de la ciberseguridad de todos los actores que participan en la generación, transmisión, distribución y consumo de la energía eléctrica.

2.3 Cadena de Bloques (Blockchain)

Las cadenas de bloque son uno de los más recientes enfoques de ciberseguridad para garantizar la confianza, integridad y disponibilidad de la información. Cuando se habla de cadenas de bloques, más del 90% de las ocasiones se asocia con el *BitCoin*: Una moneda electrónica cifrada (criptomoneda) de punto a punto y de fuente abierta. Se ha observado un uso creciente de esta tecnología como apoyo a la ciberseguridad. El desarrollo y las aplicaciones de cadenas de bloque han recibido un gran interés por parte de la comunidad investigadora durante el último lustro. Aunque no existe una definición única, la cadena de bloques se puede describir como una tecnología de red de sistema distribuido P2P, donde un repositorio de datos denominado libro mayor se comparte entre todos los nodos de la red. Las transacciones realizadas en el libro mayor son validadas por la mayoría de los nodos de la red, por lo que se ha convertido en un mecanismo de seguridad descentralizado altamente eficiente para garantizar la confianza entre todas las partes involucradas [80].

Por lo tanto, la cadena de bloques es un tipo de tecnología de libro mayor distribuido (DLT, por sus siglas en inglés). DLT es un consenso de datos replicados, descentralizados, compartidos y sincronizados distribuidos en múltiples sitios. Otros DLT son Gráficos Acíclicos Dirigidos (DAG, por sus siglas en inglés) como IOTA o BlockDAG, y HashGraph [81]. La estructura de datos de una cadena de bloques es similar a una lista enlazada donde un nuevo bloque está enlazado al bloque anterior y así sucesivamente hasta que llega al bloque génesis. El proceso forma una cadena de bloques, donde los eslabones de la cadena se construyen mediante criptografía con funciones *hash* (ver Figura **2-11**). Dado que hay funciones hash involucradas, es muy difícil manipular los datos contenidos en los nuevos bloques; manipular bloques implica cambiar todos los bloques anteriores. Esta propiedad se llama inmutabilidad y garantiza la integridad de los datos.

Figura 2-11 *Estructura de datos general básica de una cadena de bloques.*

Otra característica crucial de blockchain radica en su alta disponibilidad. Por ejemplo, con un solo nodo en la red de la cadena de bloques, la información se puede recuperar debido a que todos los nodos de la cadena de bloques contienen todas las transacciones de datos. Otra característica importante de la cadena de bloques es su transparencia, ya que puede ser auditable. En otras palabras, todas las transacciones se pueden rastrear para que cualquiera pueda verificarlas. Un bloque reúne un conjunto de transacciones de diferentes nodos de la red. Los nodos de la red distribuyen las transacciones a los otros nodos de la red para que sean verificadas, acordadas y validadas en el momento. La estructura de cada nodo es simple y generalmente tiene un identificador único seguido del hash que lo vincula al bloque anterior (nulo si es el bloque génesis) así como al conjunto de transacciones realizadas [82]. Las partes involucradas deben firmar y validar la transacción antes de que la transacción se registre en el bloque.

La parte central de una cadena de bloques es el algoritmo de consenso que define cómo varios nodos acuerdan validar las transacciones. Hay muchos algoritmos de consenso. Quizás el

algoritmo de consenso más popular sea PoW [83]. PoW, a menudo denominado minería, es un algoritmo computacionalmente intensivo que requiere una gran potencia de procesamiento y disponibilidad de memoria para resolver acertijos y validar transacciones. Se han derivado varias metodologías para adaptarse a los requisitos de procesamiento del algoritmo de PoW, incluido el equipo informático dedicado de alto rendimiento, y clusteres de equipos para lograr una mayor potencia computacional. Otras soluciones han aprovechado los múltiples núcleos de las tarjetas aceleradoras de gráficos, las nuevas arquitecturas de procesamiento paralelo, los dispositivos de matriz de puerta programable en campo (FPGA, por sus siglas en inglés) y los circuitos integrados de aplicación específica (ASIC, por sus siglas en inglés).

Debido a las limitaciones de PoW, han aparecido varios algoritmos de consenso, destacando Prueba de Participación (PoS, por sus siglas en inglés) y Prueba de Actividad (PoA, por sus siglas en inglés) de hoy, aunque hay muchos algoritmos de consenso y aún están en desarrollo [84]. En la Tabla **2-6** se mencionan los más relevantes, mientras que a continuación, se describen los más citados en la literatura. Con * se muestra la propuesta de algoritmo de consenso de este trabajo doctoral.

Tabla 2-6 *Algotimos de consensos más importantes en la literatura.*

Algoritmo	**Tipo**	**Descripción**
PoW	Basado en pruebas	Prueba de Trabajo
PoS/DPos	Basado en pruebas	Prueba de Participación / Distribuida
PoA	Basado en pruebas	Prueba de Autoridad
PoI	Basado en pruebas	Prueba de Importancia
PoET	Basado en pruebas	Prueba de Tiempo Transcurrido
PoSpace	Basado en pruebas	Prueba de Espacio
PoEf*	Basado en pruebas	Prueba de Eficiencia
PBFT	Basado en votos	Tolerancia a Fallas Práctica Bizantina
RCA	Basado en votos	Algoritmo de Consenso Ripple
FC	Basado en votos	Consenso Federado

En PoS, un nodo tiene que apostar algo que posee, generalmente en forma de criptomoneda. Si un nodo malicioso intenta manipular la cadena de bloques y otros nodos detectan el intento

de alterar la cadena de bloques, las apuestas bloqueadas se reducen o las recompensas se retienen. Otra variante de PoS es DPoS, donde los nodos de la red votan por un conjunto de nodos para que sean los delegadores [85]. PoA es una forma modificada de PoS, donde en lugar de participar con el valor monetario, la función de participación viene dada por la documentación de identidad del validador.

La gran mayoría de cadenas de bloques, como es el caso de la mayoría de las criptomonedas, son de tipo público, donde los nodos se pueden agregar fácilmente en un entorno informático abierto, sin necesidad de permisos especiales para realizar las operaciones relevantes. Por tanto, se necesitan algoritmos de consenso eficaces para garantizar la confianza entre todos los nodos [86]. Los dispositivos de IoT y SMI requieren que los algoritmos de consenso consuman pocos recursos computacionales, lo que genera un creciente interés de investigación en el desarrollo de algoritmos de consenso ligeros para dispositivos de IoT y SMI [87].

Otras de las características de la cadena de bloques de interés son los contratos inteligentes (CI), que son programas informáticos validados por la cadena de bloques que definen las reglas de operación de las transacciones. El proyecto más consolidado de cadenas de bloques con CI es Ethereum [88].

Entre los usos más frecuentes de la cadena de bloques destacan, además de la moneda virtual, el manejo de pagos seguros, autenticación en dispositivos de IoT, contratos inteligentes, voto electrónico, validación de productos como documentos, entre muchos otros [89]. Algunos beneficios son:

- Ahorro de tiempo ya que las transacciones pueden hacerse en menos tiempo garantizando confianza.
- Eliminación de costos al no haber intermediarios.
- Reducción de riesgos al evitar cibercrímenes como manipulación y fraude de la información.
- Incremento de confianza al tener un proceso compartido y rastreable.

A pesar de las ventajas que ofrece blockchain para asegurar las transacciones de datos, existen algunos inconvenientes. Por ejemplo, la naturaleza inherente de la cadena de bloques puede producir un crecimiento exponencial del tamaño de la cadena de bloques. En contraste, se ha sugerido que el crecimiento de la cadena de bloques sigue la Ley de Metcalfe, proporcional al crecimiento del hardware [90]. Otro aspecto importante a considerar es el tiempo requerido para confirmar y validar transacciones. Además, la cadena de bloques requiere una alta potencia computacional lo que implica un alto consumo de energía eléctrica que genera calor y por lo tanto no es amigable con el medio ambiente. Con respecto a la ciberseguridad, la popularidad generalizada de las aplicaciones basadas en cadena de bloques ha despertado el interés de personas malintencionadas por explotar las vulnerabilidades de la red [59] para hacerse cargo de la red, como el ataque del 51% [91], mediante el cual los nodos

corruptos pueden validar transacciones falsificadas. Es probable que el creciente interés en todo el mundo por desarrollar estrategias de seguridad basadas en blockchain atraiga más ataques y, por lo tanto, existe la necesidad de fortalecer los protocolos de seguridad.

Una de las áreas de aplicación de cadena de bloques más populares es la REI [92]. El 90% de las implementaciones de DLT se llevan a cabo a nivel de distribución de clientes. También es notorio que en la actualidad este ámbito todavía no está regulado en el mercado de la energía [93]. Dado que la adopción generalizada de soluciones de seguridad basadas en cadena de bloques es bastante reciente, faltan estándares y normas para regular el funcionamiento de los sistemas de ciberseguridad basados en blockchain. Recientemente, varias organizaciones como IEEE, Organización de Estándares Internacionales (ISO, por sus siglas en inglés) y Consorcio de Web Mundial Extendida (W3C, por sus siglas en inglés) entre otras, han comenzado a definir estándares para la interoperabilidad de las cadenas de bloque [94]. Mientras tanto, la tecnología de cadena de bloques se ha desarrollado de forma privada, mediante la cual una empresa o consorcio define las reglas para la interconexión de nodos a la red. Además, las empresas de servicios públicos administran permisos para operaciones de bloque, lo que genera cuatro tipos de cadenas de bloques para SMI: cadenas de bloques públicas sin permiso, públicas con permiso, privadas sin permiso y privadas con permiso [94].

Las cadenas de bloques pueden eliminar algunas barreras a los sistemas de energía transactiva (TES, por sus siglas en inglés). Dada su capacidad para proteger los datos de los clientes, las cadenas de bloques podrían agilizar la contratación de múltiples partes, la personalización masiva de contratos complejos y las ofertas directas entre dispositivos a nivel local. Estos elementos pueden permitir a los consumidores y productores de electricidad en el borde de la red realizar transacciones masivas entre sí [95]. Las principales aplicaciones de blockchain dentro de la REI son: Plataforma de Energía P2P, Microrrredes, Contratos Inteligentes en Mercados Eléctricos Mayoristas, Subasta de Precios de Energía, Integración con Energía Renovable, Sistemas de Distribución y Transmision, Respuesta a la Demanda, Mercados de Energía, VE, entre otros.

2.4 Mercados Eléctricos en México

La comercialización de energía eléctrica que se produce y se consume forma un complejo ecosistema denominado mercado eléctrico, en donde los diversos participantes ayudan no solo a la producción de energía eléctrica sino también en su transmisión, distribución y regulación. Las transacciones que se realizan de compra/venta están enfocadas a maximizar las ganancias de los participantes que se reflejan en mejores tarifas para los consumidores finales.

En México, la estructura del mercado eléctrico ha estado muy centralizada por parte del gobierno, pero dada la reforma eléctrica en los últimos años ha comenzado a abrirse a la iniciativa privada.

En esta sección se explica en primera instancia el comportamiento de los mercados eléctricos transactivos que son la base de los sistemas actuales de comercialización de energía para prosumidores en microrredes. Posteriormente se explican las tarifas eléctricas en México de manera simplificada.

2.4.1. Mercados Eléctricos Transactivos

En el esquema tradicional de la REI, tanto los flujos de potencia, como los pagos y datos fluyen a través de un modelo fuertemente centralizado dependiente de la empresa eléctrica; mientras que con el uso de cadenas de bloques se puede alcanzar una descentralizada, tal y como se ilustra en la Figura **2-12**. Por ejemplo, las transacciones de energía se pueden hacer de forma directa entre pequeños productores y consumidores. Todas las transacciones son almacenadas en la cadena de bloque haciendolas resistentes a pruebas de manipulación, por lo que se garantiza confianza entre las partes.

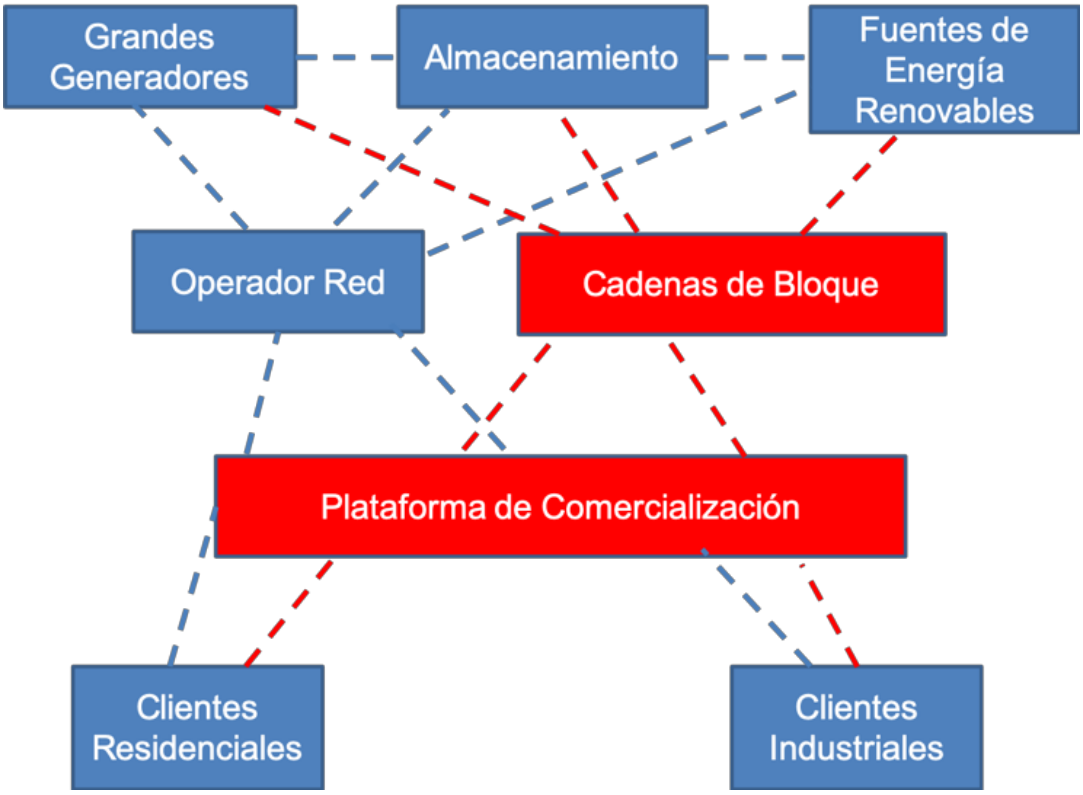

Figura 2-12 *Modelo General de Operación de Mercados Eléctricos utilizando Cadenas de Bloques.*

Dentro de la teoría de mercados eléctricos, el uso de cadena de bloques ayuda a eliminar el intermediarismo (compañías de energía, proveedores de electricidad y agregadores) haciendo que las transacciones de energía y datos se hagan de forma directa.

Los componentes de un sistema de energía basado en cadena de bloques de acuerdo con [17] son: MI, IED, Tecnologías de sensores, y Aplicaciones para teléfonos inteligentes. En la Figura **2-13**, se muestra el uso de una criptomoneda en donde a través del uso de contratos inteligentes así como de sistemas de almacenamiento de energía y MI se puede comercializar energía entre productores y consumidores de forma totalmente descentralizada.

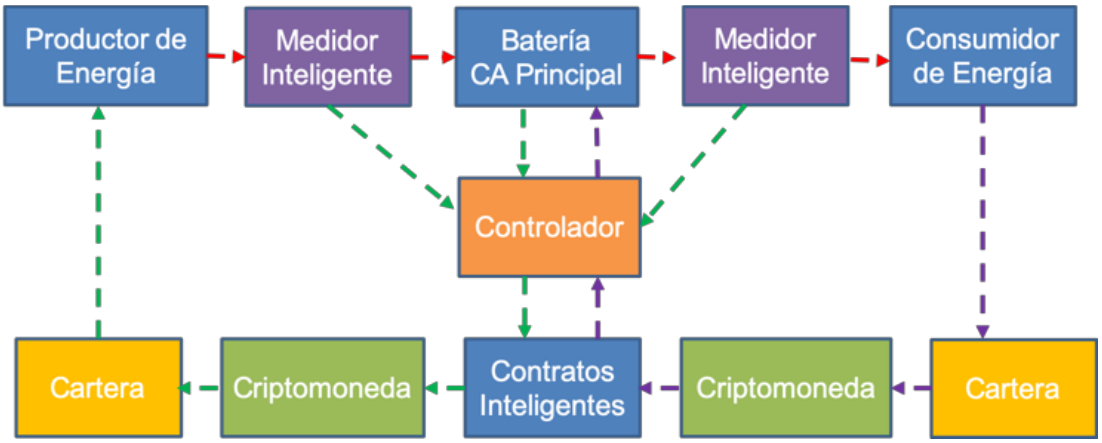

Figura 2-13 *Arquitectura General de Operación de Mercados Eléctricos utilizando Criptomonedas.*

La energía transactiva utiliza el intercambio de valor como mecanismo para gestionar mejor el flujo de energía, especialmente en el borde de la red, y se ha propuesto como una solución para comercializar energía entre prosumidores de forma descentralizada [51].

Las tendencias actuales en los mercados de la electricidad están estableciendo plataformas de cadenas de bloques y mercados minoristas en tiempo real donde los reguladores mantienen el *status quo* en las tarifas minoristas haciendo transiciones a nuevos sistemas de tarifas [96]. Estas nuevas tarifas deben adaptarse para servicios públicos regulados y no regulados y para sistemas de mercado y no basados en el mercado. Además, si la autogeneración se convierte en una forma importante de producir electricidad, las tarifas deben incluir precios de transmisión y distribución para todos los participantes.

Por otro lado, existe una desalineación entre el costo de los servicios públicos y las estructuras de tarifas, particularmente con respecto a la clase residencial. En respuesta a este desafío, muchas empresas de servicios públicos están introduciendo tasas de coste reflectantes innovadoras que se ajustan mejor tanto a sus propias necesidades como a las de

sus clientes [97]. Si bien el diseño de tarifas casi siempre implica algún grado de subsidio cruzado, las empresas de servicios públicos deben apuntar a eliminar los subsidios no intencionales entre tipos de clientes.

El éxito de implementar cualquier cambio en la infraestructura de precios requiere la satisfacción del cliente. Por el contrario, incluso si las tarifas simples se explican adecuadamente, pueden causar confusión y, posteriormente, provocar una reacción violenta de los consumidores [98]. Las nuevas tarifas deben reflejar las necesidades de los usuarios y los costos de los servicios públicos: fijos, variables y bajo demanda. Por otro lado, las tarifas eléctricas deben adaptarse a los componentes de consumo y demanda, nivel de tensión de suministro, tipo de consumo, época del año, período del día, ubicación del consumidor, entre otros factores.

Las tarifas de electricidad más comunes son el tiempo de uso (TOU, por sus siglas en inglés), el precio máximo crítico (CPP, por sus siglas en inglés), el precio máximo variable (VPP, por sus siglas en inglés) o el precio en tiempo real (RTP, por sus siglas en inglés). Los clientes del TES generalmente se suscriben a una forma de carga de referencia basada en sus patrones de uso típicos y luego compran o venden desviaciones de su referencia.

Los SMI son el componente central para medir y facturar la electricidad de acuerdo con las tarifas eléctricas, pero los nuevos esquemas de tarifas representan solo menos del 5% de los clientes [99]. Además, los SMI son una parte vital de cualquier Energía Transactiva.

2.4.2. Tarifas Eléctricas en México

Las tarifas eléctricas en México tienen una estructura escalonada según el uso (kWh), la temporada (verano o fuera de verano), la temperatura, la región geográfica, la demanda y el voltaje [100]. El período de facturación generalmente es bimestral (algunas excepciones). El principal problema de las empresas de servicios públicos, donde México no es la excepción, está relacionado con las PNT (robo, fraude y deuda) [101] y [102].

El mercado mexicano, aunque se está abriendo, sigue dominado por una empresa de servicios públicos llamada CFE. Las tarifas nacionales son 1, 1A, 1B, 1C, 1D, 1E, 1F y DAC, y dependen de la temperatura y las regiones geográficas. La Tabla **2-7** muestra las tarifas internas por temperatura mientras que la Tabla **2-8** muestra los pasos por demanda y temporada de la tarifa 1D. Los costos están en pesos mexicanos (MXN).

Cabe hacer mención que las tarifas eléctricas en México incluyen los costos de generación, transmisión, distribución, suministro, regulación, capacidad y servicios de mercado.

La Tabla **2-9** muestra las tarifas de electricidad en México fuera del verano, mientras que la Tabla **2-10** muestra las tarifas en verano. La Tabla **2-11** muestra el límite de alto consumo en cada tarifa si se excede el límite, la nueva tarifa se considera tarifa DAC (alta demanda). La Tabla **2-12** muestra las diferentes regiones y tarifas según áreas geográficas.

Tabla 2-7 *Estructura de tarifas eléctricas por temperatura.*

Tarifa	1	1A	1B	1C	1D	1E	1F
Temperatura promedio	<25C	25C	28C	30C	31C	32C	>=33C

Tabla 2-8 *Ejemplo de tarifas escalonadas y costos de energía en tarifa 1D en Región Centro Occidente.*

Temporada	Escalón	Costo por kWh	kWh de consumo
Fuera de verano	Básico	$0.81	Primeros 75 kWh
	Intermedio	$1.00	Siguientes 125 kWh
	Excedente	$2.91	Cada kWh adicional
Verano	Básico	$0.72	Primeros 175 kWh
	Intermedio bajo	$0.81	Siguientes 225 kWh
	Intermedio alto	$1.07	Siguientes 200 kWh
	Excedente	$2.87	Cada kWh adicional

Tabla 2-9 *Tarifas eléctricas fuera de verano.*

Tarifas	1	1A	1B	1C	1D	1E	1F
Consumo básico los primeros	75 kWh	75 kWh	75 kWh	75 kWh	75 kWh	75 kWh	75 kWh
Consumo intermedia los primeros	65 kWh	75 kWh	100 kWh	100 kWh	125 kWh	125 kWh	125 kWh
Excedente de consumo	140 kWh	150 kWh	175 kWh	175 kWh	200 kWh	200 kWh	200 kWh

Tabla 2-10 *Tarifas eléctricas en verano.*

Tarifas	1	1A	1B	1C	1D	1E	1F
Consumo básico los primeros	75 kWh	100 kWh	125 kWh	150 kWh	175 kWh	300 kWh	300 kWh
Consumo intermedia los primeros	65 kWh	50 kWh	100 kWh	150 kWh	225 kWh	450 kWh	900 kWh
Consumo intermedio los siguientes	NA	NA	NA	150 kWh	200 kWh	150 kWh	1300 kWh
Excedente de consumo	140 kWh	150 kWh	225 kWh	450 kWh	600 kWh	900 kWh	2500 kWh

Tabla 2-11 *Límte de alto consumo.*

Tarifa	1	1A	1B	1C	1D	1E	1F
Límite	250 kWh	350 kWh	500 kWh	850 kWh	1000 kWh	2000 kWh	2500 kWh

Tabla 2-12 *Tarifas por regiones y Estados.*

#	Division	Estados
1	BC	Baja California
2	BCS	Baja California Sur
3	Noroeste	Sonora y Sinaloa
4	Norte	Chihuahua y Durango
5	Golfo Norte	Coahuila, Nuevo León y San Luis Potosí
6	Centro Golfo	Tamaulipas
7	Jalisco	Jalisco, Nayarit
8	Bajío	Zacateca, Guanajuato, Aguascalientes, y Querétaro
9	Valle de México Norte	Hidalgo y Estado de Mexico

10	Valle de México Central	Ciudad de México y Estado de Mexico
11	Valle de México Sur	Morelos
12	Centro Occidente	Michoacán y Colima
13	Centro Este	Puebla
14	Esrte	Veracruz
15	Sureste	Oaxaca, Chiapas y Tabasco
16	Peninsular	Yucatán, Quinta Roo, y Campeche

Capítulo 3 Desarrollo del Proyecto

En el presente capítulo se desarrolla la metodología propuesta de este trabajo de investigación.

Se presentan las etapas de análisis, diseño e implementación de la solución propuesta.

3.1 Conceptualización de los SMI dentro de una arquitectura borde-niebla-nube

Como se describió en el capítulo 2, la arquitectura de cómputo distribuido borde-niebla-nube se ha empezado a utilizar en diversos sistemas ciberfísicos particularmente en la REI. Una de nuestras aportaciones (que han empezado a manejar otros autores) ha sido describir a los SMI dentro de una arquitectura distribuida de borde-niebla-nube como se visualiza en la Figura **3-1**.

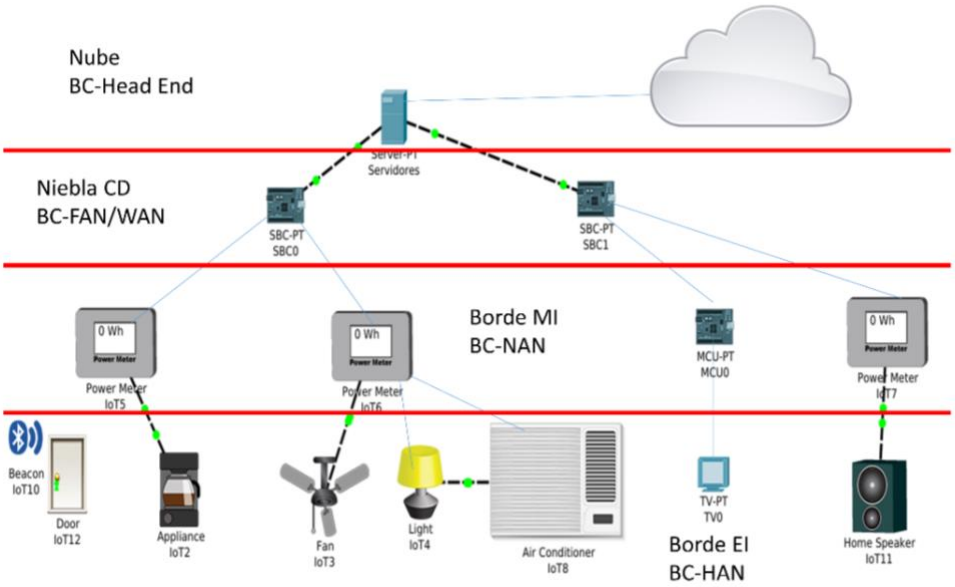

Figura 3-1 *Un SMI dentro de una arquitectura borde-niebla-nube.*

Como se puede apreciar, nuestra capa de borde está conformado por nuestros MI que pueden comunicarse con los electrodomésticos, sistemas DER y otros IED a través de redes cableadas como Ethernet o Comunicación en Líneas de Potencia (PLC, por sus siglas en inglés). A su vez la capa de niebla está conformada por los CD que puedan estar interconectados de forma adyacente en área geográficas cuya separación puede ser variable dependiendo de las necesidades de la empresa eléctrica. Finalmente, la capa de la nube hace referencia a los centros de datos de las empresas de servicios públicos que pueden interconectarse entre sí a través de nubes públicas o privadas haciendo uso de Internet.

3.2 Análisis de Riesgos en SMI

Es importante realizar el análisis de vulnerabilidades presentes en los SMI, en los cuales a través de la revisión de la literatura del estado del arte se pudo caracterizar la parte de ciberseguridad presentada previamente en los capítulos 1 y 2 de este trabajo. Como se mencionó, es sumamente importante seguir un SGSI ya que reúne las mejores prácticas, recomendaciones y estándares en el establecimiento de ciberseguridad de forma metodológica. La parte fundamental de cualquier SGSI consiste en la realización de un análisis de riesgo que permita determinar cuál es el estado actual de los activos de información para establecer políticas y objetivos de ciberseguridad que permitan garantizar la protección de la información y su constante monitoreo.

Para el análisis de riesgos, es necesario evaluar los factores internos y externos de la organización para cada activo; además de los roles de los involucrados en los procesos. Tradicionalmente, el análisis de riesgos se ha centrado en las amenazas y vulnerabilidades que forman parte de los activos de información

Aunque existen muchos marcos de evaluación y gestión de riesgos, en este trabajo se definió una metodología propia de análisis de riesgos simple para evaluar activos con base en las premisas básicas de la ciberseguridad: CIAS, revisando el impacto que cada uno de ellos puede causar. La Tabla **3-1** muestra cómo se asigna una puntuación a cada activo de seguridad de la CIAS.

Tabla 3-1 *Calificación de riesgo para cada premisa de ciberseguridad.*

Valor	**Marcador**
Alto	3
Medio	2
Bajo	1

Para cada activo, las amenazas, vulnerabilidades, contramedidas e impactos se consideran determinando el riesgo para cada elemento de la CIAS. Los resultados de la ponderación se

dan como la suma de la puntuación de cada premisa. La Tabla **3-2** muestra la puntuación total para la evaluación de riesgos de un activo.

Tabla 3-2 *Marcador Total para evaluación de riesgo de un recurso.*

Marcador Total	**Valor**
7-9	Alto
5-6	Medio
3-4	Bajo

Antes de realizar el análisis de riesgos, es necesario considerar los distintos tipos de procesos y flujos de negocios del problema a resolver. A continuación, se muestran los diferentes escenarios de posibles vulnerabilidades.

El escenario 1 descrito como Caso general, se muestra en la Figura **3-2**. En este caso se describe las fallas existentes dentro de la arquitectura de un SMI separándolo por las capas de borde-niebla-nube.

En la capa de borde, los puntos más susceptibles de fallas son el prosumidor, los dispositivos inteligentes, los DER, así como las diveras redes de comunicación, además de los MI en su software. En la capa de niebla, los puntos vulnerables se centran también en los MI en su comunicación con otros MI y CD, los CD en su software, así como la comunicación de CD con otros CD y los servidores de la empresa eléctrica. Finalmente, en la capa de nube las vulnerabilidades se focalizan en los sistemas de información y base de datos principalmente.

En el escenario 2 descrito en la Figura **3-3**, el usuario/cliente revisa su historial de consumo y facturación a través de la Web o aplicación móvil. Otro subcaso consisten en mostrar la información visual de su consumo. Aquí, los puntos de falla son las aplicaciones móviles y Web (los responsables son los programadores de la empresa eléctrica), Internet y otras redes, servidor Web, MDBS y Facturación (administrador de sistemas son los responsables).

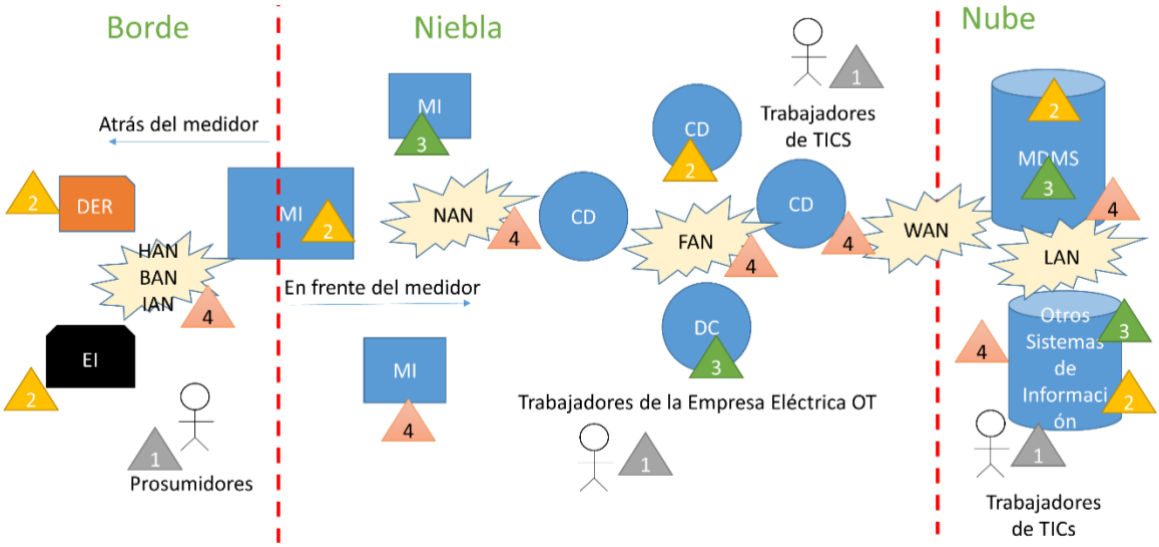

Figura 3-2 *Escenario general del funcionamiento de un SMI mostrando sus diversos puntos de falla.*

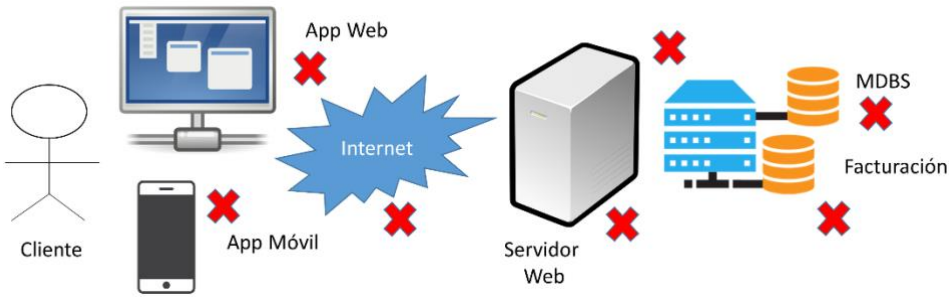

Figura 3-3 *Uso del portal del SMI.*

Una variante del escenario dos es el pago de consumo eléctrico a través del portal (ver Figura **3-4**). Para este sub caso, los clientes deben estar autenticados en la aplicación Web o móviles. Se requerirá el número de cliente y contraseña para acceder a las aplicaciones, por lo que será necesario que el usuario construya una contraseña segura y robusta, periódicamente se debe cambiar la contraseña además de no compartirla. Además, los clientes deben almacenar y proteger la información de su tarjeta de crédito. Estas actividades son ejemplos de operaciones de ciber higiene que deben realizar los clientes. Entre las vulnerabilidades se encuentran: usuarios malintencionados que quieren suplantar identidad para el robo de información, seguridad en redes de telecomunicaciones y la interconexión con los sistemas bancarios para el pago en línea.

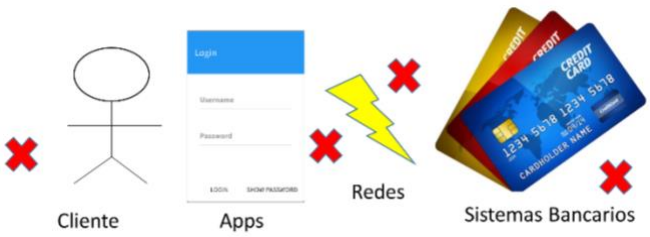

Figura 3-4 *Subcaso 2.1 pago de consumo eléctrico.*

Por último, otro de los casos de interés radica en la comunicación de las lecturas del MI a través de toda la infraestructura de los SMI para llegar a los MDMS de la empresa eléctrica. La Figura **3-5** muestra este escenario, en donde se visualizan las diversas vulnerabilidades de manera general, siendo las más comunes el hardware y software de MI y CD, la interconexión de los datos, la seguridad física de los MI y CD, así como la seguridad de los sistemas de información y de BD.

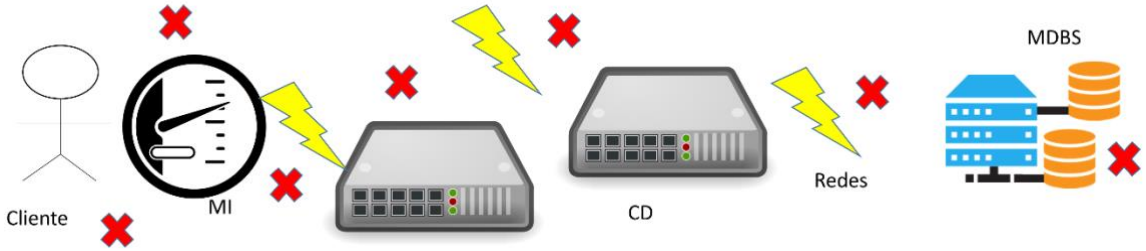

Figura 3-5 *Escenario 3 de comunicación de lecturas de medición de los MI a través del SMI.*

Finalmente, se realizó el análisis de riesgos en SMI a través de las capas borde, niebla y nube.

En la capa de borde, el principal activo es el MI, donde la principal amenaza son las personas malintencionadas. Debido a que todas las instalaciones de la CIA están comprometidas, el riesgo es alto. El MI es el elemento crucial en el SMI, y su ciberseguridad es crítica porque su impacto es la reputación de la empresa de servicios públicos.

En la capa de niebla, el principal activo es el CD, donde la principal amenaza son las condiciones climáticas. Un CD con condiciones climáticas extremas no puede operar, y las

instalaciones de la CIA se ven comprometidas. El riesgo se considera alto porque su impacto es mayor. El CD concentra la información de los bloques en el vecindario, y un mal funcionamiento impacta en las mediciones y facturación del consumo/producción eléctrica.

Por último, en la capa de la nube, el principal activo es el MDMS, donde la principal amenaza son los ataques de hackers a través de aplicaciones Web o móviles que se conectan a los servidores de bases de datos del MDMS. El riesgo es extremadamente alto debido a que las instalaciones de la CIA se ven comprometidas, y la reputación de las empresas de servicios públicos puede verse afectada.

3.3 Arquitectura de una cadena de bloques multinivel para SMI

La arquitectura propuesta se basa en la arquitectura AMI adaptándose a la arquitectura de cómputo distribuida borde-niebla-nube descrita en la sección 3.2. La arquitectura propuesta para proteger los datos de medición se muestra en la Figura **3-6**.

Se puede apreciar que conceptualmente se tienen al menos 4 cadenas de bloques (BC1, BC2, BC3, BCn) representando las áreas de HAN/BAN/IAN (aunque este trabajo se centra en HAN), NAN, FAN/WAN (que pueden crecer de forma variable dependiendo de la densidad de CD y a su extensión geográfica), y finalmente, el Head-End (representando por el centro de datos de la empresa eléctrica).

En HAN, existen EI (SA en inglés) que permiten medir su consumo energético y reportarlo al MI para generar una cadena de bloques por hogar, oficina o industria. El consumo de todos los electrodomésticos convencionales se almacena en el MI. Otro componente importante son los DER que permiten producir energía. El excedente de producción de energía se inyecta en la red y la transacción se guarda en la cadena de bloques.

La red de MI está dentro de NAN. Tenga en cuenta que cada MI está asociado con una HAN particular y que todos los MI están asociados con un CD. En NAN se forma otra blockchain con los datos de todos los MI de la red. Los datos almacenados aquí son solo un resumen de los datos de cada MI ya que la privacidad de los datos debe protegerse a toda costa.

La Figura **3-7** muestra que el MI y el CD necesitan una BD para almacenar los datos de las transacciones realizadas. La BD del CD es mayor que el del MI y SA. La cadena de bloques propuesta en varios niveles se utiliza para garantizar la seguridad de los datos.

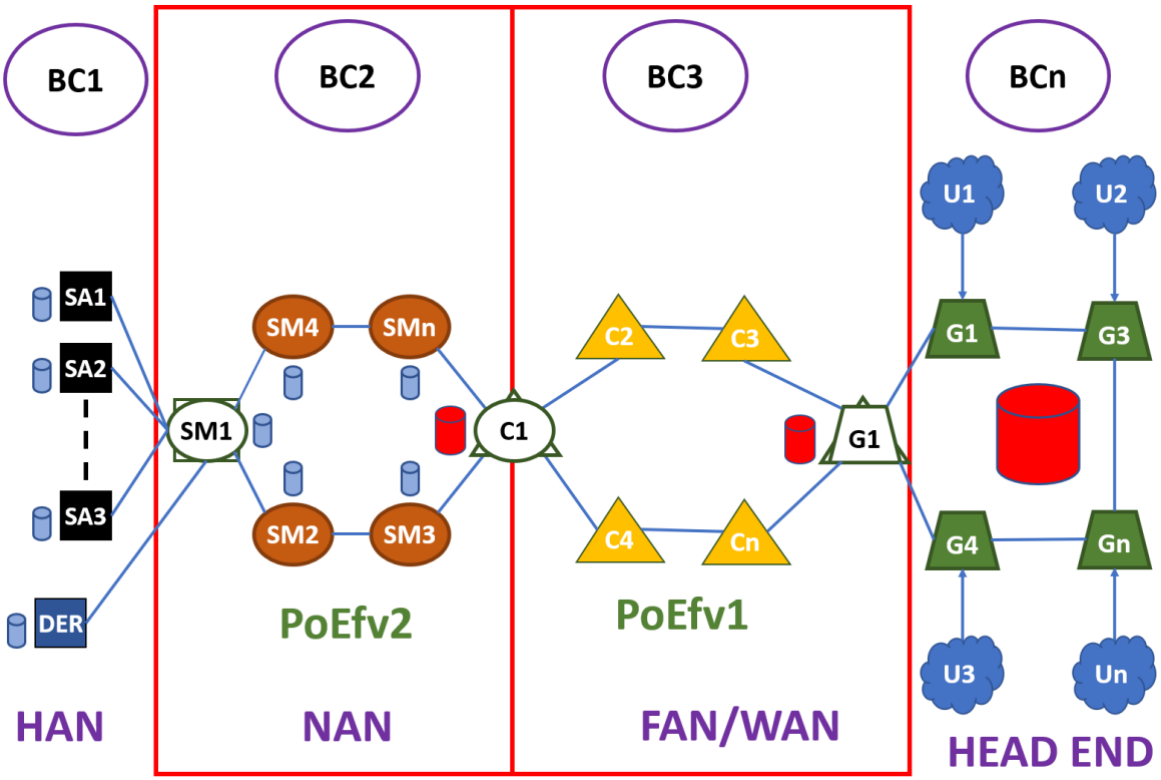

Figura 3-6 *Arquitectura propuesta basada en las cuatro áreas elementales deAMI.*

Nótese que todos los niveles en la arquitectura de almacenamiento de datos usan una cadena de bloques. En este caso, EI, MI, y CD tienen BD. De manera general los datos que se almacenan son los valores de la señal eléctrica, particularmente los registros de consumos y producción se guardan como transacciones en la cadena de bloques, más adelante en esta misma sección se describen las estructuras de datos manejadas en cada capa.

El siguiente nivel de la arquitectura está en FAN/WAN donde el CD resume los datos de cada WAN y por lo tanto requiere una mayor capacidad de almacenamiento. Finalmente, en los servidores de la empresa eléctrica, los datos de todos los clientes se almacenan en una cadena de bloques que puede ser interoperable con otras empresas de servicios públicos.

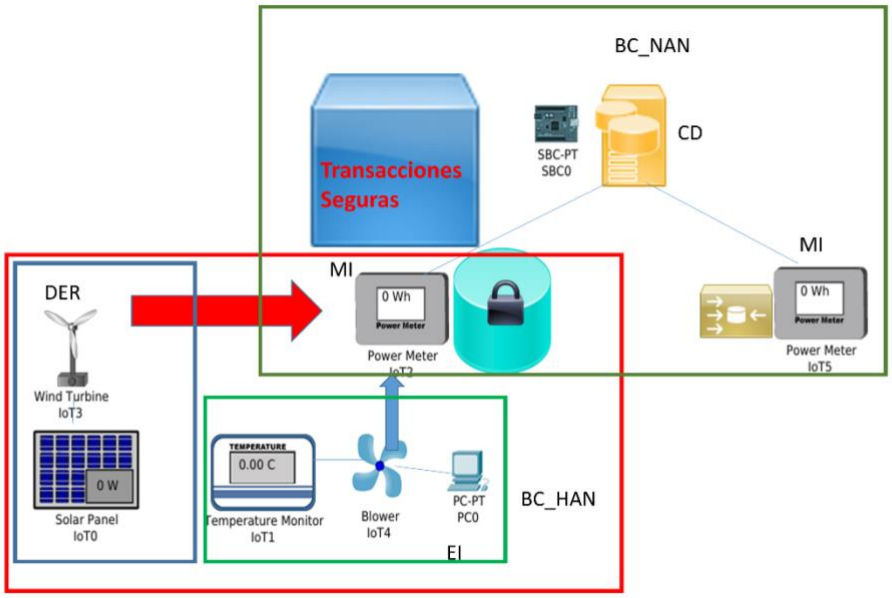

Figura 3-7 *Almacenamiento de datos general de la arquitectura de cadena de bloques propuestas.*

A continuación, se describe el flujo de trabajo de toda la arquitectura:

1) Blockchain en HAN (Nivel 1)

Todos los dispositivos eléctricos consumen energía eléctrica y el MI mide el consumo de energía de estos dispositivos conectados en la HAN. Además, el MI mide la producción de energía de DER. En el caso de las SA y DER, es importante que incluyan una base de datos embebida para almacenar su propio consumo/producción de energía ya que, con esto, se podrá realizar una cadena de bloques. La estructura de datos en este nivel de la cadena de bloques se muestra en la Figura **3-8**. Notese que solamente EI y DER con BD embebida hacen una cadena de bloques.

En este nivel, para cada hogar, una cadena de bloques representa todo el consumo/ producción de energía para los dispositivos en cada hogar (E, EI y DER). El funcionamiento de las cadenas de bloques es muy similar en todos los niveles.

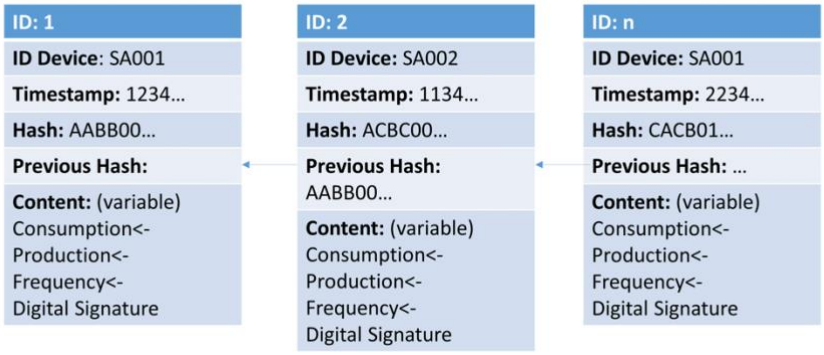

Figura 3-8 *Estructura de datos Blockchain implementada en el nivel HAN.*

2) Blockchain en NAN (Nivel 2)

El MI reporta información concentrada sobre el consumo/producción de todos los dispositivos en HAN y resume un bloque con esta información en forma de transacción de energía. Esta transacción de energía se firma entre el MI y la empresa eléctrica para pasar a la cadena de bloques y realizar su validación.

Las transacciones en SMI pueden ser, además de lecturas de medida y producción de energía eléctrica, eventos de conexión/reconexión, alarmas y cualquier otra situación que sea reportada en los logs de los MI o que sea notificada por la empresa eléctrica (por ejemplo, precios dinámicos o eventos de respuesta a la demanda, entre otros). La estructura de datos de la cadena de bloques en este nivel se muestra en la Figura **3-9**. Tenga en cuenta que cualquier bloque tiene un número variable de transacciones. El contenido de cada transacción también es variable. Cada bloque está vinculado a un bloque anterior mediante su valor hash.

Al momento de firmar la transacción, se agrega una prosa legal que funciona como una especie de CI, donde se indicará en texto claro la transacción que se está realizando. La Figura **3-10** muestra un ejemplo de prosa legal, donde los campos en negrita muestran los datos a reemplazar de una manera específica. La marca de tiempo se coloca cuando la transacción se valida por la red de una cadena de bloques. Nótese que todas las palabras en en negritas son remplazadas por los datos de transacción específica.

Una vez firmadas las transacciones de cada MI, se difundirán a través de la red de la cadena de bloques. Se propuso un algoritmo de consenso llamado Prueba de eficiencia (*PoEf*) para validar transacciones. Las transacciones con mayor eficiencia energética serán recompensadas. Por ejemplo, un MI cuyo consumo real sea menor que su consumo en los

periodos anteriores podría obtener un descuento en su precio de facturación. Más adelante se describe el funcionamiento del algoritmo de consenso.

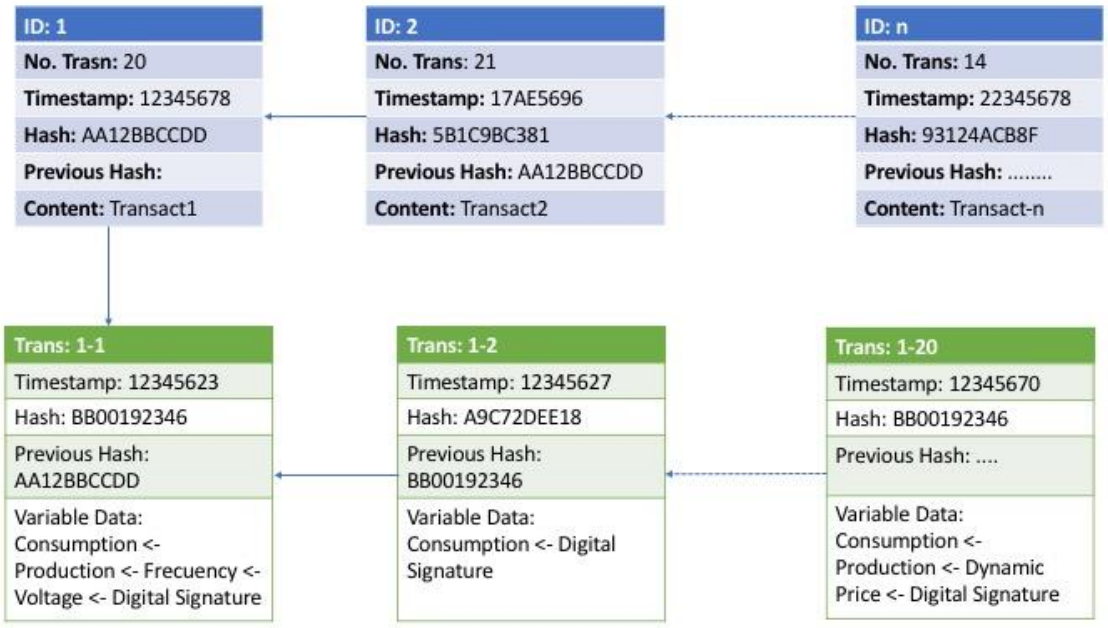

Figura 3-9 *Estructura de datos de la cadena de bloques implementada en el nivel NAN.*

Los autores proponen un período de tiempo de 15 minutos para validar transacciones en este nivel de blockchain debido a que un período de tiempo de 15 minutos es el tiempo más común para la presentación de informes de datos en AMI. La descripción de PoEf se detalla en la siguiente subsección.

El estímulo del algoritmo de consenso es una recompensa económica en su consumo (paga menos en consumo paga más en producción). El algoritmo debe ser lo más justo posible para que en un período de facturación la gran mayoría de los nodos puedan recibir esta contribución. Una vez alcanzado el consenso, se envía la solución a los demás nodos para que la agreguen a su cadena de bloques y sigan las operaciones normales de las transacciones realizadas.

This document states that the ***consumer consumed / produced x*** amount of energy, in a period of ***n*** minutes, to the **utility**, with the following quality parameters:

frequency: ***f***

voltage: ***v***

current: ***c***

power: ***p***

This transaction was signed between the parties ***date-time***

Time-stamp

Figura 3-10 *Ejemplo de una prosa legal.*

Una parte esencial de la propuesta es la gestión de un nodo coordinador en cada nivel de la cadena de bloques. El coordinador es el encargado de reportar un bloque condensado de la cadena de bloques de su red NAN al siguiente nivel (esto se repite en los otros niveles de la cadena de bloques hasta llegar al nivel final en el centro de datos). En el caso de la cadena de bloques en el nivel HAN, el coordinador del nodo es el MI. En este nivel (cadena de bloques en NAN) está el CD. En la cadena de bloques en el nivel FAN/WAN hay otro CD (la descripción del proceso de selección para el coordinador de nodos se describe en la siguiente sección).

3) Blockchain en FAN/WAN (Nivel 3 a N-1)

En este nivel, la cadena de bloques está formada por todos los CD de una región. Depende de la densidad de los nodos o de las distancias entre los nodos cuántos niveles de cadenas de bloques adicionales se deban implementar. La Figura **3-11** muestra el bloque condensado de las transacciones en este nivel de la cadena de bloques. Tenga en cuenta que cualquier bloque tiene un número variable de transacciones y contenido. La información adicional sobre eventos se almacena en la cadena de bloques.

La selección del coordinador de nodo se selecciona a través de sus capacidades de hardware. La primera vez que la cadena de bloques comienza a funcionar, se selecciona el coordinador del nodo. Todos los nodos están numerados para funcionar como mecanismos de respaldo.

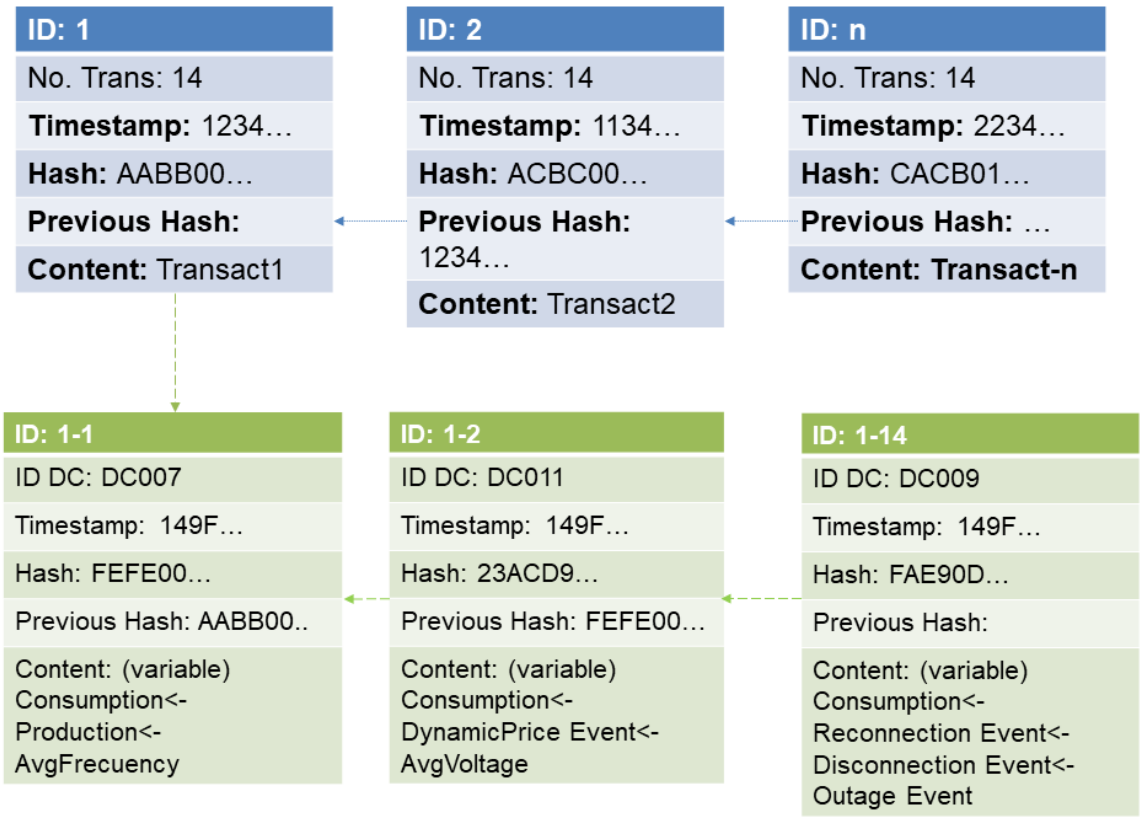

Figura 3-11 *Estructura de datos de la cadena de bloques implementada a nivel FAN / WAN.*

En este nivel de la cadena de bloques, se propuso una modificación del algoritmo PoEf para demostrar las capacidades de la arquitectura propuesta relacionadas con las capacidades de modificación de parámetros en cada nivel de la cadena de bloques. El período para el algoritmo de consenso en este nivel se seleccionó en 10 minutos debido al aumento en el volumen de datos a procesar.

Después de un tiempo, los nodos en cada cadena de bloques (excepto el nivel final donde siempre está toda la cadena) limpiarán su espacio de almacenamiento, debido a la limitación de espacio en disco (principalmente en EI y MI). El coordinador es responsable de registrar

los diferentes eventos de blockchain, incluidos los eventos de espacio limpio y fallas de coordinación.

La Figura **3-12** muestra el proceso para limpiar un nodo de blockchain en cualquier capa de la arquitectura propuesta. En el paso 1, el nodo envía un mensaje a su coordinador y construye una base de datos temporal para las transacciones entrantes (paso 2). El coordinador almacena este evento en la cadena de bloques (paso 3) y envía un evento de limpieza a los otros niveles de las cadenas de bloques (paso 4). Finalmente, cuando se limpia la base de datos anterior, la base de datos temporal se renombra como la base de datos principal (paso 5). Tenga en cuenta que este proceso es el mismo en todos los niveles de la arquitectura propuesta.

Figura 3-12 *El proceso de limpieza de un nodo de la cadena de bloques.*

Cuando se agregan nuevos nodos a la red, deben tener su cadena de bloques parcial hasta el momento en que comiencen a funcionar. Los nuevos nodos que se incorporan a la red comienzan a operar en cadena alterna mientras se descarga la cadena de trabajo original, una vez descargada esa génesis de bloque inicial de la segunda cadena de bloques se une con el último eslabón de la cadena. Cuando un nodo de nivel superior reintegra la cadena, no es necesaria una nueva sincronización.

La Figura **3-13** muestra el proceso cuando se agrega un nuevo nodo a cualquier capa de la arquitectura propuesta. Primero (paso 1), el nuevo nodo envía un mensaje al coordinador (previamente el coordinador ha sido notificado por la empresa eléctrica de los nuevos nodos

que se agregarán). El coordinador confirma la adición del nuevo nodo y éste comienza a descargar la base de datos de la cadena de bloques (paso 2) y construye una base de datos temporal cuando se están almacenando las nuevas transacciones (paso 3), posteriormente el coordinador envía la información de que hay un nuevo nodo a los otros nodos (paso 4), y finalmente, el coordinador envía el evento de un nuevo nodo agregado a los siguientes niveles. Nótese que este proceso es el mismo en todos los niveles de la arquitectura propuesta.

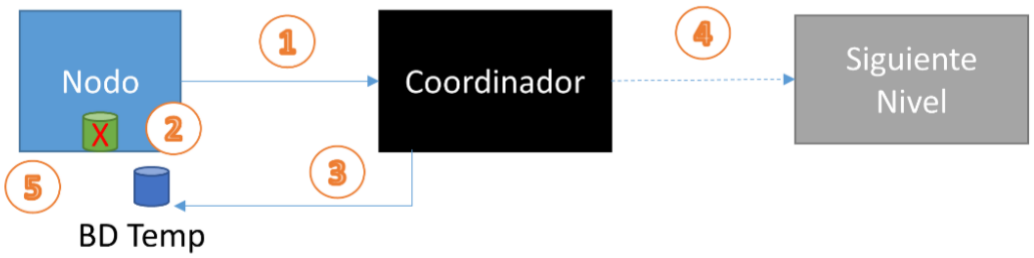

Figura 3-13 *Proceso de adición de nuevos nodos.*

El nodo coordinador tiene un mecanismo de respaldo de tal manera que, si falla, el segundo nodo de respaldo entra a trabajar. En caso de que falle el segundo mecanismo de respaldo, los nodos de la cadena de bloques pueden continuar trabajando registrando la información. Tan pronto como se reinstale el nodo coordinador, las cadenas de bloques se completarán como en cualquier otro nodo que haya salido o ingresado a la red. El CD debe informar los bloques resumen de su red si no se han enviado.

4) Blockchain en el centro de datos (Nivel N)

En este nivel, todos los servidores de cabecera en AMI concentran todas las transacciones en los diferentes niveles de cadenas de bloques. Esta cadena de bloques podría ser enorme y los datos nunca se eliminan como una cadena de bloques tradicional. La Figura **3-14** muestra la estructura de datos de la última y principal cadena de bloques de nivel. Tenga en cuenta que este nivel tiene toda la información y nunca deja caer su información.

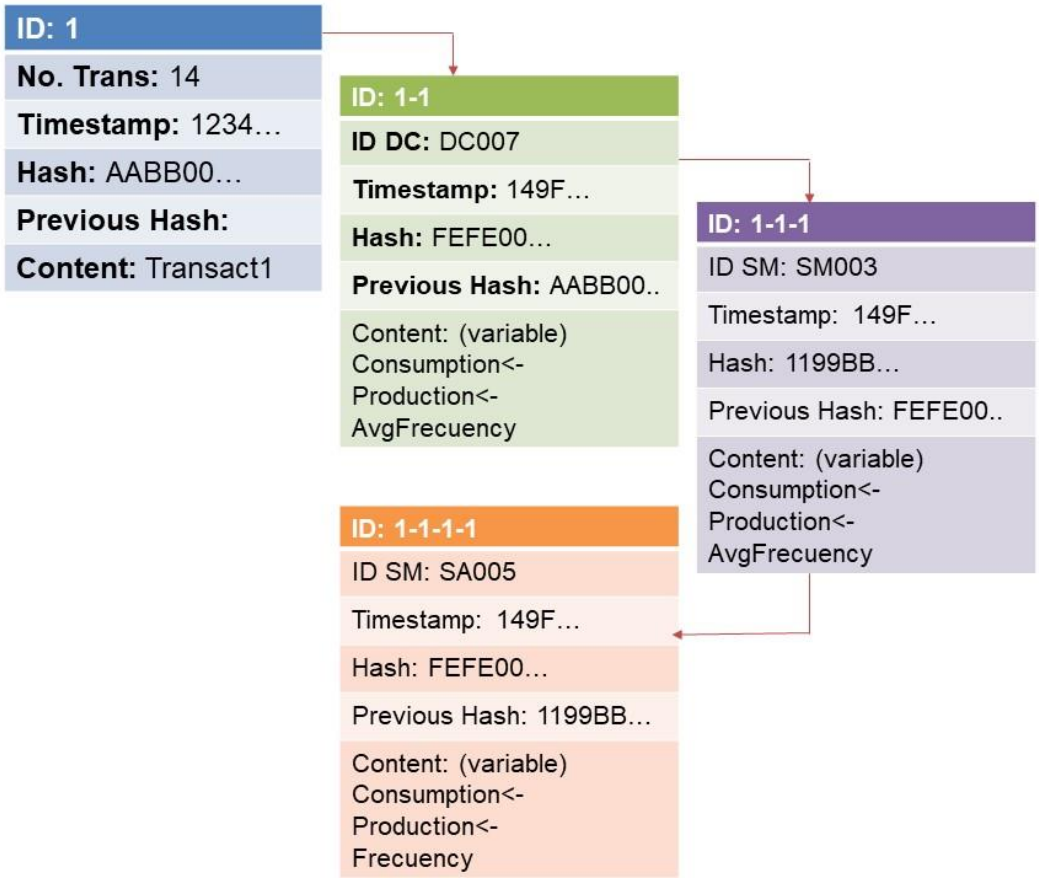

Figura 3-14 *La estructura de datos completa de Blockchain en el último nivel.*

3.4 Algoritmo Prueba de Eficiencia (PoEf) versión 1

Este algoritmo se implementa en los distintos niveles de la cadena de bloques considerando las características de cada nivel. En particular, se describirá su implementación en HAN, en la que se premiará a los nodos que hayan tenido el mejor consumo energético en función de su desempeño anterior (haciendo analítica de datos en la cadena de bloques).

El análisis de datos se realiza dentro de la cadena de bloques en el período particular buscando patrones de consumo (verificando la eficiencia energética) y producción de energía (considerando factores como la calidad de la energía producida).

Se considera que se descartan todas las transacciones de producción de energía que no cumplan con los parámetros de calidad energética (se puede adaptar para darles un cierto valor económico).

La descripción de la versión 1 básica del algoritmo PoEf se presenta a continuación (ver Algoritmo 1), en donde:

R_c = tasa actual,

P_c = producción actual,

C_c = consumo de corriente,

R_l = última tasa,

P_l = última producción,

C_l = último consumo,

R_p = tasa anterior,

per = período de tiempo de la transacción,

L = límite del período inicial,

n = número total de períodos,

R_a = tasa promedio,

P_{per} = producción de período específico,

C_{per} = consumo de un período específico,

R_{amax} = tasa promedio máxima,

R_{cmin} = tasa de corriente máxima,

R_{lmin} = última tasa máxima.

El algoritmo PoEf en la versión 1 básica calcula los mejores nodos de eficiencia energética (MI) en tres momentos: actual, anterior y promedio (esto puede ser adaptable). Además, PoEf calcula una previsión del período de facturación actual en función de los períodos de facturación anteriores. Los nodos más eficientes son recompensados con un porcentaje de descuento de su tarifa de facturación en ese período. Esto recompensa a los prosumidores con una mejor eficiencia energética en su consumo/producción de electricidad.

Algoritmo 1 *Proof-of-Efficiency Version 1 básica*

Entrada: Un conjunto de transacciones de energía

Requerimientos: todos los nodos tienen el mismo conjunto de transacciones

1: Actualizar las transacciones de lecturas en la BD

2: **Para** todos los nodos presentes en the la transacción actual **Entonces**

3: $R_c = P_c - C_c$

4: $R_l = P_l - C_l$

5: $R_p = R_c - R_l$

5: **Para** $per=L$ **Hasta** $per= n-2$ **Entonces**

6: $R_a = promedio(P_{per} - C_{per})$

7: **Fin Para**

8: $R_{amax} = max(R_a)$

9: **Fin Para**

10: $R_{cmax} = max(R_c)$

11: $R_{lmax} = max(R_l)$

Salida: el conjunto de nodos con la eficiencia máxima, previa y tarifa promedio

La versión 1 extendida del algoritmo PoEf verifica la base de datos completa para hacer un pronóstico sobre el consumo/producción de energía utilizando un enfoque estadístico de series de tiempo con el algoritmo Modelo Autoregresivo Integrado de Promedio Móvil (ARIMA, por sus siglas en inglés). La versión 1 extendida del algoritmo PoEf se implementó utilizando la biblioteca *statsmodels* en lenguaje Python. Esta versión del algoritmo de consenso tiene un mecanismo de detección de patrones de consumo que puede ayudar a determinar posibles robos de energía o mal funcionamiento de los instrumentos de medición. El responsable de cada dispositivo es el MI.

En general, el algoritmo de consenso propuesto se basa en PoA con una mezcla de PoW. Los nodos pueden iniciar ataques, pero el esquema de seguridad debe completarse con otras medidas y controles de seguridad.

Las ventajas de la arquitectura de cadena de bloques multinivel propuesta son las siguientes:

1. La segmentación en varios niveles de la arquitectura propuesta ayuda a mejorar la eficiencia del almacenamiento de datos porque la cadena de bloques es extremadamente grande. Además, la segmentación de la arquitectura de varios niveles propuesta ayuda a almacenar datos solo donde es necesario, lo que permite la privacidad de los datos.
2. Tener capas segmentadas permite realizar aplicaciones más directas sobre la información y los datos generados. Por ejemplo, dentro de la cadena de bloques en HAN, los electrodomésticos están conectados al MI, de modo que se puede obtener información desglosada por consumo de energía por electrodoméstico. No obstante, en la cadena de bloques HAN, el concentrador de datos puede optimizar el consumo de energía de todo el vecindario; mientras que en FAN/WAN la red de concentradores puede ayudar en el consumo eficiente de energía en un área grande como una ciudad o región.
3. Otra ventaja de la implementación multicapa es que se pueden ejecutar varios algoritmos de consenso optimizados para las capacidades computacionales de cada nivel de la cadena de bloques. Por ejemplo, PoEf en HAN, se puede adaptar para medir la eficiencia energética de cada SA, mientras que en FAN/WAN se puede medir la eficiencia energética de un vecindario o región específica. El algoritmo dentro de HAN debería enfocarse más en la baja capacidad de cómputo de EI, mientras que en FAN/WAN los concentradores tienen mayor poder de cómputo.
4. El tiempo utilizado en los algoritmos de consenso se puede modificar en cada capa. Por ejemplo, se utilizó HAN porque es el tiempo promedio en el que se realizan los reportes de medición en AMI, pero este parámetro se puede adaptar a tiempos mayores o menores. Lo importante a nivel NAN es que estos tiempos se pueden diferenciar en cada NAN para que se opere de forma diferente en el siguiente nivel FAN/WAN.
5. La arquitectura propuesta es capaz de diferenciar y priorizar eventos que requieren atención inmediata pensando en aplicaciones futuras como la gestión de cortes de energía o fallas de suministro. Cada capa puede tener más de un tiempo para el algoritmo de consenso según el tipo de evento.
6. El uso de la prosa legal permite que el compilador de CI sea lo suficientemente ligero como para adaptarse fácilmente a cualquier dispositivo dentro de SMI.

Las desventajas de la arquitectura propuesta son:

1. En realidad, la arquitectura propuesta se implementa en hardware específico (detallado en el siguiente capítulo). Mucho de los MI utilizados hoy en día son heredados, por lo que es necesario agregar módulos de hardware y software para intentar lograr la interoperabilidad entre la mayoría de las implementaciones reales de AMI.
2. La propuesta arquitectónica podría introducir algunos riesgos de ciberseguridad que en el capítulo 4 se analizan con más detalle. Asimismo, se presenta cómo se propone la arquitectura para solucionar las amenazas y vulnerabilidades en SMI.

También en el siguiente capítulo se describe cómo la arquitectura propuesta responde a otros problemas como gastos generales, rendimiento y escalabilidad.

3.5 Algoritmo Prueba de Eficiencia (PoEf) versión 2: Sistema de Análisis de Datos Multinivel para SMI

Está basado en la arquitectura borde-niebla-nube descrita en la sección anterior. El nivel de borde está representado por EI, DER y MI. En la actualidad, los EI y DER rara vez se consideran porque no incluyen capacidades de hardware para procesar y almacenar datos. Sin embargo, debido a las tendencias actuales en el desarrollo de dispositivos IoT, se considera que la introducción comercial de dispositivos EI con mayores capacidades de IoT, almacenamiento y procesamiento de datos proliferará durante la próxima década y, por lo tanto, es importante abordar la importancia de EI y DER, como parte de la arquitectura general. De manera similar, los MI incluyen regularmente una capacidad de almacenamiento BD embebida limitada y capacidades limitadas de procesamiento de datos. El nivel de niebla está representado por CD que procesan datos en tiempo real obtenidos del MI. El nivel de nube está representado por MDMS y la infraestructura de TIC de todas las empresas de servicios públicos para almacenar y procesar macrodatos. La arquitectura propuesta se muestra en la Figura **3-15**.

La arquitectura propuesta comprende cuatro áreas principales de comunicación de datos AMI (HAN, NAN, FAN/WAN, Head-End) en 3 secciones. La sección 1 es el nivel de borde. La sección 2 representa los niveles de niebla. La sección 3, compuesta por la cabecera, representa el nivel de nube. Las áreas delimitadas por cuadrados representan cargas (E, EI, DER); los círculos representan MI, los triángulos representan CD, los cilindros representan BD, los trapezoides representan los Servidores Gateway (G) de la empresa de servicios públicos y las nubes representan las redes de comunicación de datos externas de las otras empresas de servicios públicos. La Analítica en el Borde (EA por sus siglas en inglés) está representado dentro de cada MI y la Analítica en la Niebla (FA por sus siglas en inglés) está

representado para cada CD. La comunicación de datos entre cada componente de la arquitectura se realiza a través de la misma red y protocolos de comunicación de datos. El análisis de datos se realiza en el nivel más cercano. En la EA, el análisis de datos se realiza en línea utilizando la transmisión de datos para procesar diferentes aplicaciones de análisis de datos.

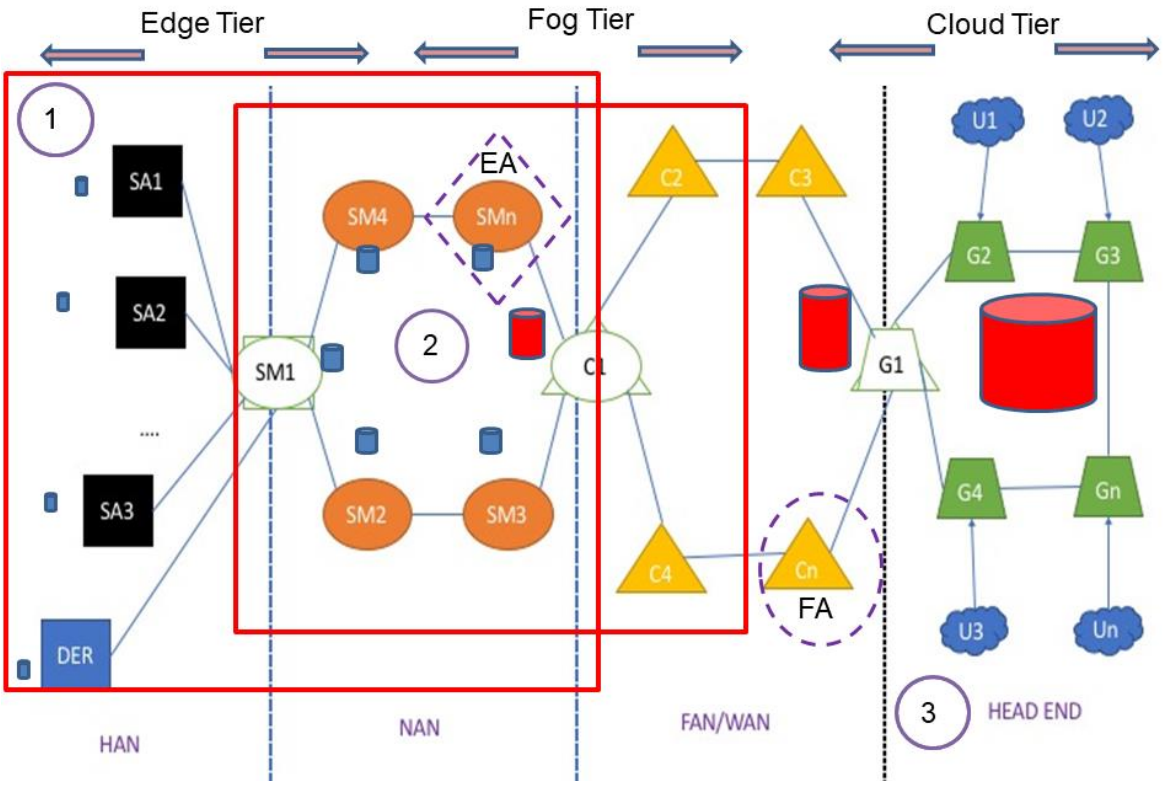

Figura 3-15 *Diagrama de alto nivel de la arquitectura propuesta.*

La arquitectura utiliza aprendizaje automático (ML, por sus siglas en inglés de *Machine Learning*) para calcular los nuevos parámetros de las diferentes aplicaciones de análisis de datos de acuerdo con las capacidades computacionales utilizando Aprendizaje por Reforzamiento (RL, por sus siglas en inglés de *Reinforcemnet Learning*). RL es una especie de proceso de aprendizaje basado en retroalimentación. Los alumnos aprenden por ensayo y error. RL es un conjunto formado por agentes, entornos, acciones y recompensas [103]. La implementación de RL de este trabajo se basa en un proceso de decisión de Markov (MDP, por sus siglas en inglés).

MDP es una tupla M = <S, A, Φ, R> compuesta por:

- Un conjunto finito de Estados S, (si ∈ S, i = {1, ..., N}).
- Un conjunto finito de Acciones A, que dependen de cada estado (aj (si), j = {1, ..., M}).
- Una función de recompensa R, que define el objetivo y la asignación de cada acción de estado a un número (recompensa), que indica los estados deseables (f (s, a) ⇒ R).
- Un modelo de entorno o función de transición de estado Φ (s '| s, a) (Φ: A × S → S) que indica la probabilidad de alcanzar el estado s' ∈ S cuando la acción a ∈ A se completa en el estado s ∈ S.

Además, un modelo MDP utilizado en RL requiere tres características principales:

- Política (π): define el comportamiento del sistema en el dominio del tiempo y consiste en mapear (a veces estocástico) los estados de las acciones (π (S) → A).
- Función de valor (Vf): indica lo que es bueno a largo plazo y corresponde a la recompensa total que un agente podría esperar para acumular. El estado inicial de la función es s (Vf (s)) o un estado que actúa a (Q (s, a)).
- Las recompensas las da el medio ambiente, pero los valores deben estimarse (aprender) en función de las observaciones. El proceso de aprendizaje se define como a Q Vf π (s) = max Q π (s, a).

Los agentes son los procesos que se ejecutan en los MI, CD y Servidores de la empresa eléctrica. Los entornos dependen de las diferentes variables de cada aplicación de análisis de datos en la arquitectura propuesta. Las acciones corresponden a las diferentes tareas para predecir, clasificar, actividades de aprendizaje. Constantemente, la arquitectura monitorea los diferentes estados de los algoritmos de análisis de datos. Las recompensas son los valores que optimizan los diferentes algoritmos de análisis de datos en la arquitectura propuesta según las políticas. Las políticas y las funciones de valor intentan minimizar o maximizar el rendimiento de la aplicación analítica de datos. La arquitectura es flexible y cada nivel se puede utilizar como una variante de algoritmos para el análisis de datos. La Figura **3-16** muestra el procedimiento de aprendizaje.

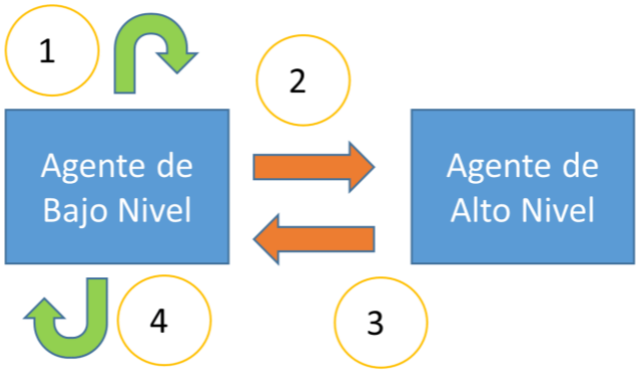

Figura 3-16 *El aprendizaje por reforzamiento en la arquitectura propuesta.*

El proceso comienza en el nivel inferior del Agente. El Agente en los niveles inferiores (Al) ejecuta sus aplicaciones de análisis de datos y evalúa su política (π) y la función de valor correspondiente (Vf) para estimar si el nuevo estado (S) tiene una mejor recompensa (R) usando sus parámetros locales. A continuación, el Al emite una solicitud al Agente en el nivel superior (Au) preguntando sobre los parámetros globales de sus vecinos. En consecuencia, Au informa los parámetros a la Al que emitió la solicitud. Finalmente, la Al ajusta sus parámetros de acuerdo con la nueva información y evalúa si los parámetros actualizados tienen una mejor recompensa.

Los niveles inferior y superior dependen del contexto actual de la aplicación de análisis de datos en la arquitectura. La combinación de niveles inferiores y superiores podría ser (SA / DER => MI), (MI => CD), (CD => CD) y (CD => G), que son los niveles inmediatos, pero todos los niveles están conectados directamente entre sí. Por ejemplo, los MI (nivel de borde) son retroalimentados directamente por CD (nivel de niebla) e indirectamente por G (nivel de nube). La segmentación de la arquitectura en niveles permite un mejor rendimiento de la analítica de datos de acuerdo con las capacidades de hardware de cada dispositivo, utilizando los datos cuando se necesitan en el momento que se requiera.

La plataforma de análisis de datos multinivel para SMI se probó para tres aplicaciones analíticas de datos: pronóstico del consumo de energía, predicción de la calidad de la energía y predicción del robo de energía. A continuación, se describen cada una de las aplicaciones.

a) Pronóstico de Consumo de energía

En general, el procesamiento de análisis de datos para pronosticar el consumo de energía se lleva a cabo en el nivel del centro de datos y requiere capacidades de procesamiento de datos considerables para implementar métodos de pronóstico que van desde series de tiempo y modelos econométricos hasta algoritmos de inteligencia artificial. Se propone que el uso de datos derivados de MI y CD puede mejorar la previsión del consumo de energía. Además, la metodología propuesta da como resultado un algoritmo bastante simple que se puede implementar en la arquitectura de computación de borde y niebla propuesta. La Figura **3-17** describe el procedimiento de pronóstico del consumo de energía.

El proceso comienza en el nivel del MI, el cual procesa los datos medidos utilizando el método de series de tiempo, basado en un modelo previamente entrenado. El modelo se entrena utilizando los datos correspondientes a un día (MI en estado de medición inactivo). El MI compara continuamente los datos procesados con las predicciones, ajustando el modelo en función de los errores delta.

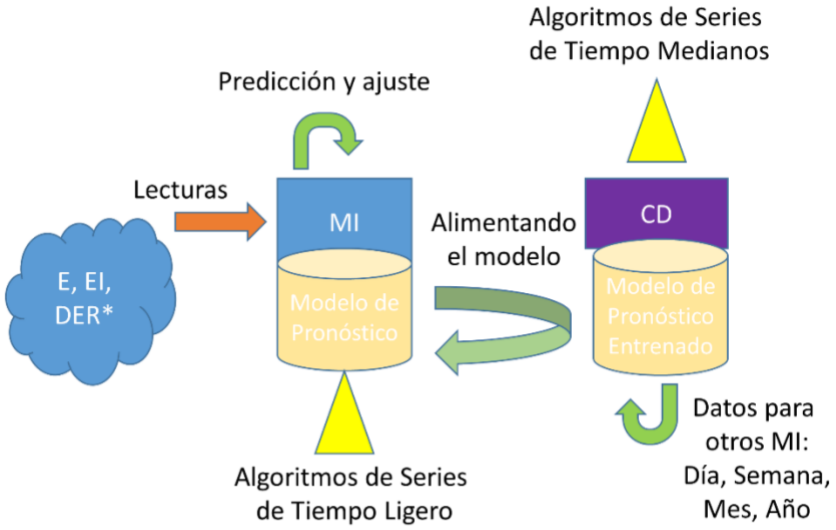

Figura 3-17 *Arquitectura para pronóstico de Consumo y Producción.*

Los algoritmos de series de tiempo utilizados en CD son más complejos que en el MI. En este caso, se utilizó el algoritmo Media Móvil Integrada Autorregresiva Estacional con Variables Externas (SARIMAX, por sus siglas en inglés). La curva de serie de tiempo resultante se compara utilizando el algoritmo de Box-Jenkins, ajustando la mejor curva al

modelo ARIMA. Luego, MI y CD ajustan los parámetros *p*, *q*, y *d* del modelo ARIMA utilizando métricas de precisión del modelo de regresión como: error cuadrático medio (MSE, por sus siglas en inglés), criterio de información de Akaike (AIC, por sus siglas en inglés) o criterio de información bayesiano (BIC, por sus siglas en inglés). Los datos derivados de la predicción basada en modelos (quince minutos, día, semana, mes y año) permiten pronosticar antes de que ocurra el evento y ajustar los modelos. La descripción de este componente se muestra en el Algoritmo 2.

Algoritmo 2 *Pronóstico de Consumo y Producción de Energía.*

Entrada: Series de Tiempo de Consumo/Producción de Energía

1: **Si no** existe un modelo preentrenado OR el modelo preentrenado es obsoleto **Entonces**

2: calcular Nuevo modelo ARIMA (p, d, q)

3: **Fin Si**

4: delta_Error <- predicción del siguiente valor – dato observado

5: **Si** delta_Error >= +/- 0.05 **Entonces**

6: contador_anomalía <- contador_anomalía +1

7: **Fin Si**

8: **Si** contador_anomalía > 5% total datos **Entonces**

9: modelo <- obsoleto

10: **Fin Si**

Salida: modelo preentrenado válido ajustado con la nueva entrada

b) Predicción de la calidad de la energía

La predicción de la calidad de la energía es una tarea compleja porque los eventos en tiempo real tienen una profunda influencia en la confiabilidad de la predicción; los eventos suelen ser rápidos y escasos, lo que impide un análisis eficaz de los datos entrantes [104]. La Figura **3-18** muestra el proceso de predicción de la calidad de la energía que se lleva a cabo en la arquitectura propuesta.

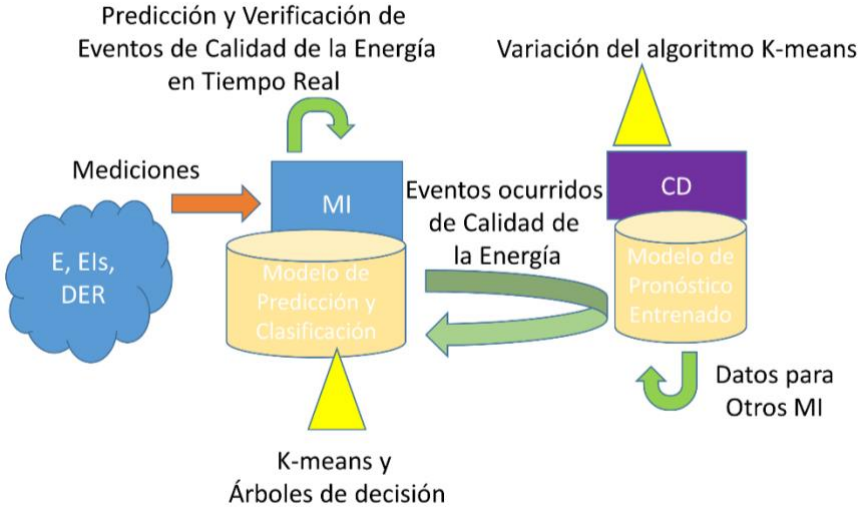

Figura 3-18 *Arquitectura para clasificación y predicción de calidad de la energía.*

El SM adquiere y procesa las mediciones de E, EI y DER. Los valores medidos (voltaje y frecuencia) son evaluados y comparados con eventos de calidad de energía estándar tales como subtensión, sobretensión, *swags* (caídas) y *swells* (ver Tabla **3-3**, [105]).

Se utiliza un árbol de decisiones para clasificar los eventos. La metodología resultante puede clasificar eventos rápidamente. Las variables de interés para el clasificador son voltaje y frecuencia. Los valores de referencia son 127V y 60Hz para voltaje y frecuencia, respectivamente. El algoritmo para clasificar datos en MI se muestra en el Algoritmo 3.

Además, el MI usa datos históricos para intentar predecir un evento de calidad de energía. El modelo de predicción es complementario con CD. El algoritmo utilizado en CD es una variación del agrupamiento de *k-medias*. El uso de la agrupación en clústeres en CD hace que sea fácil predecir dónde se encuentran los eventos de calidad de energía más comunes en el tiempo en el vecindario y puede correlacionarlos con la posición geográfica de MI. Esto puede ayudar a prevenir algunas perturbaciones generales en la red de distribución.

Tabla 3-3 *Clases de Eventos de Calidad de la Energía.*

	Magnitud pico⇓	**1 – 3 segundos**	**3 segundos – 1 minuto**	**> 1 minuto**
Variación de Voltaje	< 0.1 pu	Interrupción momentaria	Interrupción temporal	Interrupción sostenida
	0.1 – 0.8 pu	*Sag* momentario	Sag temporal	
	0.8 – 0.9 pu			Bajo voltaje
	1.1 – 1.2 pu	*Swell* momentario	Swell temporal	Sobre voltaje
	1.2 – 1.4 pu			
	< 60 Hz <	Desviación de frecuencia		
	Duración ⇒	Corta	Mediana	Larga

Algoritmo 3 *Clasificador usando Árbol de Decisión*

Entrada: frecuencia (*f*), voltaje (*v*), tamaño de ventana (*w*, default *w* = 60 segundos)

1: **Para** i=1 to *tamaño (w)* **Entonces**

2: Verificar *v* y *f*

3: **Si** v and f están en niveles anormales **Entonces**

4: *actualizar Vv(i) or Vf(i) de acuerdo con su árbol de decisión*

5: **Fin Para**

6: contar V*v* y V*f* y actualizar C*t* en estados continuos

Salida: V*c* vector de estado de voltajes, V*f* vector de estado de frecuencia, C*t* tabla de clasificación

c) Detección de Robo de Energía

Las PNT son un gran desafío para las empresas de servicios públicos. La PNT más importante es el robo de energía, que puede resultar de la manipulación de MI o la conexión a las líneas de distribución. Para diseñar este componente se utilizan los resultados de la aplicación del método de pronóstico del consumo de energía como se describió en el apartado a) de esta sección. Los resultados se utilizan para calcular un modelo para predecir un consumo anormal que podría clasificarse como robo de energía.

La Figura **3-19** muestra la arquitectura propuesta para clasificar diferentes casos de robo de energía. De manera similar a la previsión del consumo de energía, el MI analiza los datos informados por los dispositivos eléctricos y compara las lecturas de datos con el comportamiento previsto. Si la anomalía continúa por un período determinado, se marca como posible robo de energía y se informa al MI y a la empresa eléctrica.

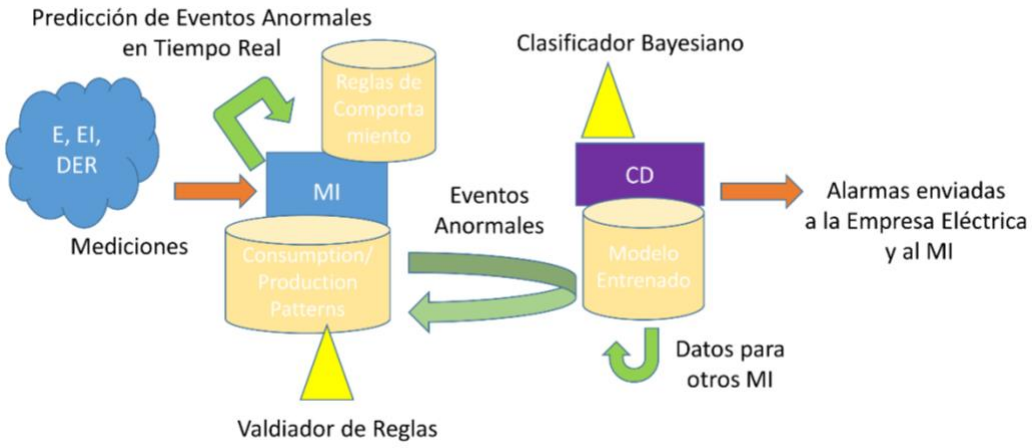

Figura 3-19 *Arquitectura para predicción de robo de energía.*

Teniendo en cuenta que la mayoría de los eventos de robo de energía se pueden clasificar como eventos probabilísticos, el algoritmo implementado en este nivel es un clasificador bayesiano (ver Algoritmo 4).

Algoritmo 4 Clasificador de predicción de robo de Energía

Entrada: *Deltas* de consumo/producción de energía predichas y reales, tamaño de la ventana de evaluación (*w*, default *w* = 60 minutos), % límie de variación (*lv*, default *lv*=10%), y el promedio de eventos de calidad de la energía en el CD.

1: **Para** i=1 to *tamaño (w)* **Entonces**

2: Verificar *deltas* de consumo/producción *de energía* y comparar con periodos previos

3: **Si** *deltas* >= *lv* **Entonces**

4: *v* := *true*

5: **Para Si**

6: Verificar eventos de calidad de la energía en el MI y comparar con el CD

7: Construir un *árbol de probabilidad* con los eventos en MI

8: **Fin Para**

9: **Si** *v* = *true* **Entonces**

10: recorrer el *árbol de probabilidad* y calcular las correlaciones con eventos de calidad

10: **Si** *correlación* de *eventos* < 0.5 **Entonces**

11: *probabilidad = 1 – (probabilidad * deltas)*

10: **Fin**

11: *probabilidad = deltas (porcentaje)*

Salida: % probabilidad de robo de energía

3.6 Algoritmo Prueba de Eficiencia (PoEf) versión 3: Sistema Transactivo de Energía

Un modelo de Energía Transactiva (TE, por sus siglas es inglés) está compuesto por dos elementos: mecanismos de control y de mercado con el propósito de equilibrar dinámicamente la oferta y la demanda. En la Figura **3-20** se muestra un modelo general de energía transactiva basado en mercados minoristas de electricidad. En donde además de los

participantes tradicionales (incluyendo prosumidores) se encuentra la plataforma de energía transactiva.

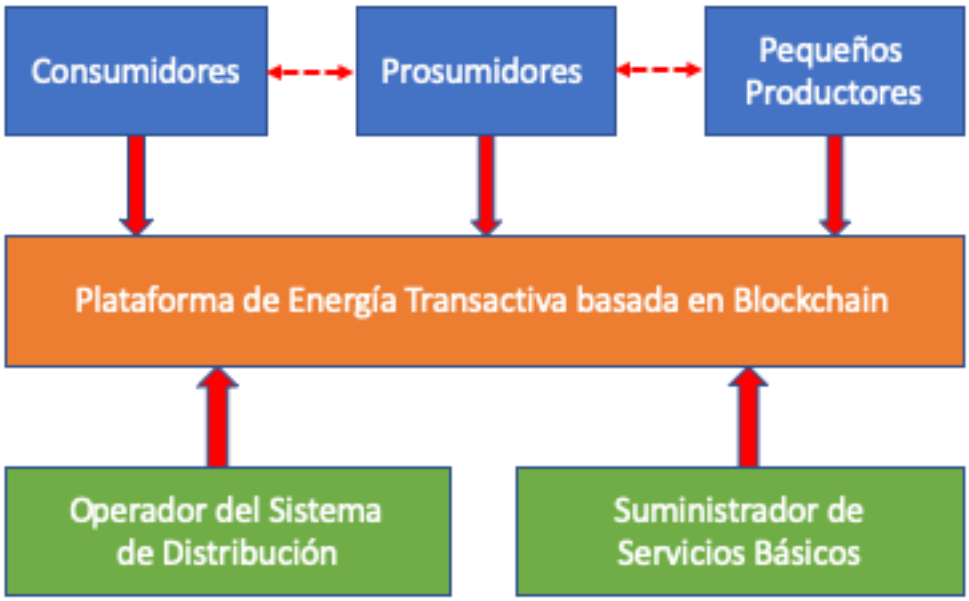

Figura 3-20 *Modelo Propuesto de Mercados Eléctrico Minorista Transactivo.*

La Plataforma de Energía Transactiva contiene además de componentes de la cadena de bloques dos elementos primordiales: un sistema de almacenamiento de datos masivos con su respectivo módulo de analítica de datos e interfaces de comunicación hacia otros componentes del mercado eléctrico no tan presentes en el mercado minorista como los comercializadores y agregadores más comunes en el mercado eléctrico mayorista, tal y como se muestra en la Figura **3-21**.

En la Figura **3-22** se muestra de manera general la interacción de cada actor participante en el mercado eléctrico transactivo con sus componentes principales.

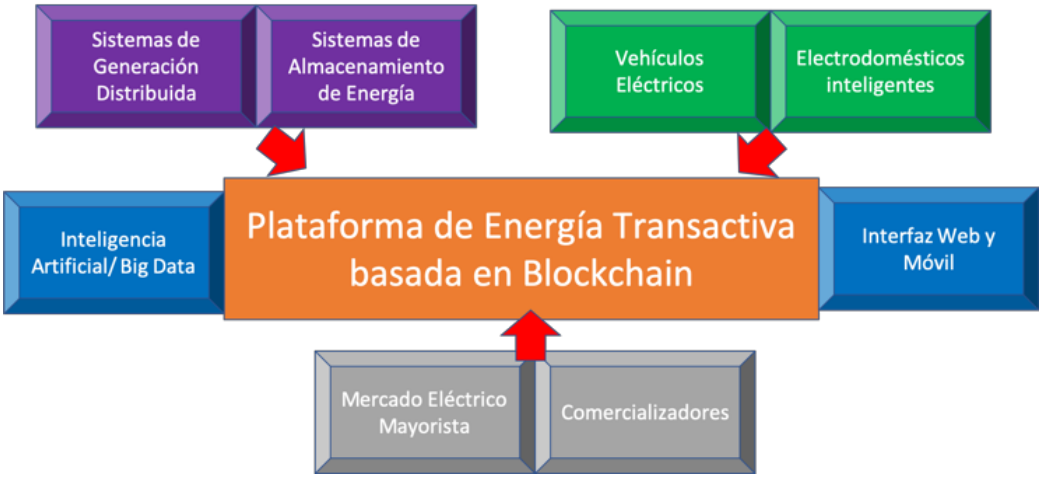

Figura 3-21 *Interfaces de la plataforma de energía transactiva propuesta.*

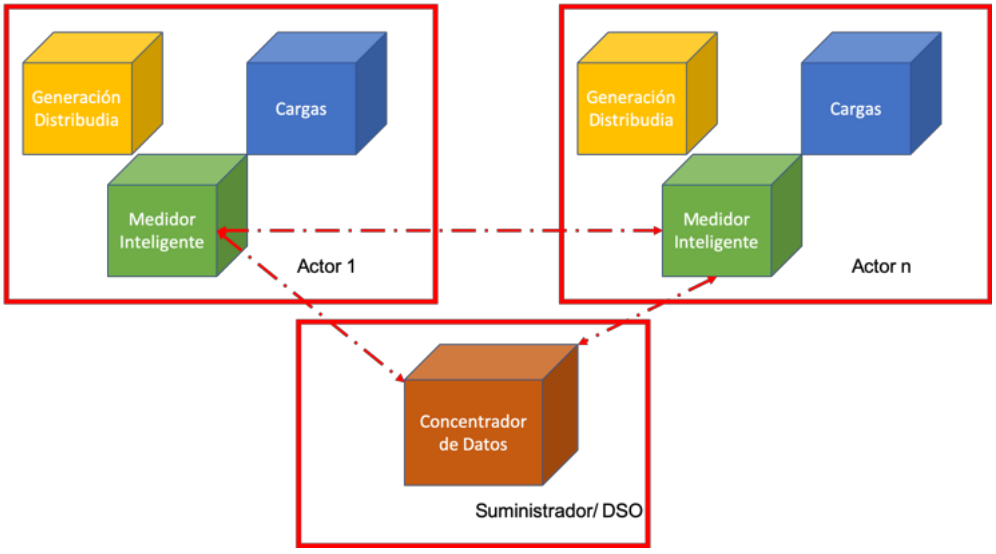

Figura 3-22 *Interacciones de la plataforma de energía transactiva propuesta.*

La arquitectura está basada en los dos modelos previos de PoEf (Arquitectura multinivel de cadenas de bloques y de analítica de datos en sistemas de medición) y es una continuación con la mejora del modelo TE. La arquitectura general de TES usando cadena de bloques y la infraestructura de SMI se presenta en la Figura **3-23**. Observe que, en este trabajo, cada nivel de la arquitectura de SMI se adaptó a una arquitectura de computación distribuida en la nube-niebla-borde.

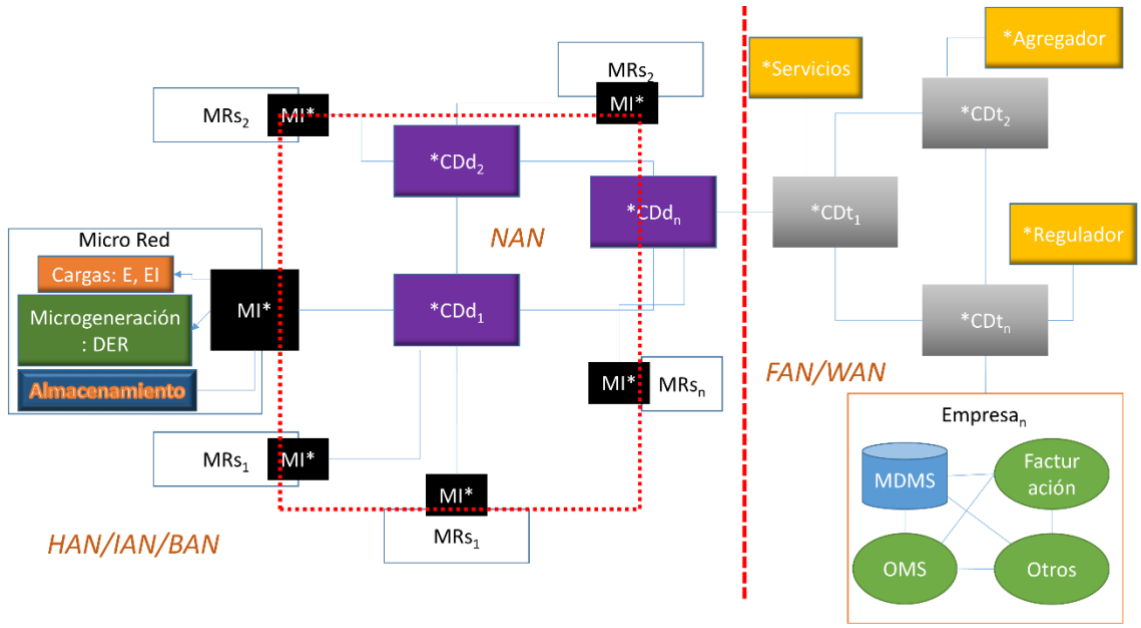

Figura 3-23 *La Arquitectura de Sistema de Energía Transactiva usando SMI y cadena de bloques.*

La arquitectura del SMI se divide en tres grandes partes al igual que los modelos previos corresponden a las capas de borde (HAN), niebla (NAN/FAN) y nube (FAN/WAN). Como elemento adicional se tiene contemplado un sistema de almacenamiento de energía.

Todos los dispositivos y partes con * tienen TES usando blockchain. La Microrred (MG, por sus siglas en inglés) puede estar con diferentes proveedores e interconectada a través de MI y CD. La parte NAN está compuesta por MI y CD. El CD puede ser integrado por diferentes Operadores de Sistemas de Distribución (DSO, por sus siglas en inglés) representados como CDdn. La parte FAN/WAN está compuesta por el último CD donde se pueden interconectar diferentes Operadores del Sistema de Transmisión (TSO, por sus siglas en inglés) representados como CDtn. Otros participantes que se pueden interconectar en esta parte son Agregadores, Reguladores, Servicios, Empresas Eléctricas, entre otros. Dentro de las Empresas Eléctricas, el TES se puede interconectar con diferentes sistemas de Tecnologías de la Información (IT, por sus siglas en inglés) y Tecnologías Operativas (OT, por sus siglas en inglés) como el MDMS, Facturación, Sistemas de Gestión de Cortes (OMS, por sus siglas en inglés), entre otros.

La Figura **3-24** muestra una descripción detallada de la arquitectura TES en el dispositivo MI. Observe en la parte inferior las tres partes mencionadas en el MG: Almacenamiento, Cargas y DER. En el medio está la capa de software representada por la interfaz gráfica de usuario (GUI, por sus siglas en inglés) y el aprendizaje automático (ML) / analítica de datos (DA). En la parte superior se encuentran los otros componentes principales de un TES, el Calendarizador y Temporizador, la interconexión con el operador de la red, y finalmente, el módulo de Comercialización de Energía responsable del registro de las transacciones de energía entre los prosumidores y otros participantes del mercado.

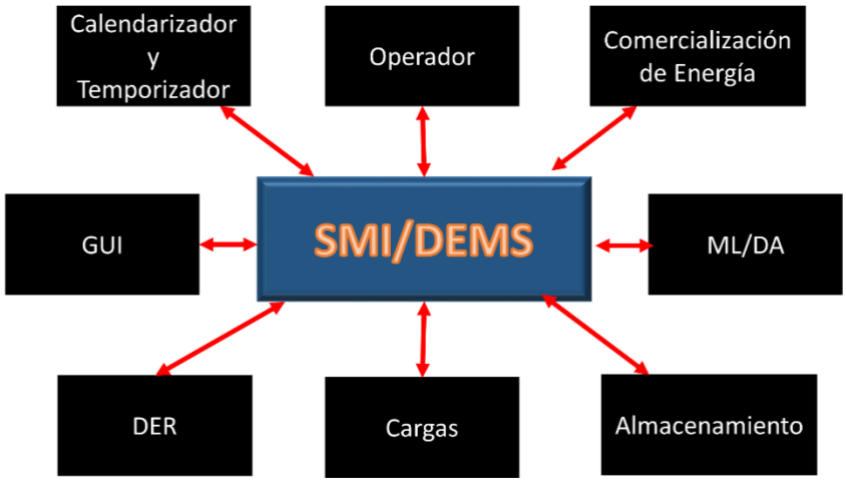

Figura 3-24 *Arquitectura TES en profundidad.*

La idea general de TE es equilibrar los mercados regulados con la reducción de los picos y llenar los valles. TE generalmente es un modelo complejo porque los mercados de energía incluyen muchas variables independientes y causalidades que son difíciles de modelar. Esta complejidad se refleja en las tarifas eléctricas que son difíciles de entender para el prosumidor en la mayoría de los casos. Se simplificó este modelo para mejorar las tarifas eléctricas y promover la eficiencia energética entre los prosumidores. Conceptualizamos simplemente un TE como se describe en Ecuación 2.

$$TE = Señales\ Economicas + Incentivos - Costos \qquad (2)$$

Ecuación 2 *Definición de Energía Transactiva.*

A continuación, describimos cada uno de los componentes principales de TE: señales económicas, incentivos y costos.

Las señales económicas vienen dadas por las condiciones de oferta y demanda de los mercados eléctricos. En particular, las condiciones de oferta y demanda aseguran que las señales económicas estén orientadas a diferentes escalas de tiempo, por ejemplo, en tiempo real para la micro generación y en el mediano y largo plazo para los mercados mayoristas de energía. Las señales están relacionadas con la compra, venta, almacenamiento o desconexión de la red para que el SEP pueda funcionar correctamente. En general, los SMI tratan elementos y mecanismos de control para garantizar la correcta ejecución de las señales económicas.

Los incentivos son otorgados por elementos provistos por el gobierno y/o empresas de servicios públicos a través de esquemas de reducción de tarifas por parte de políticas gubernamentales como subsidios en temporadas de calor o frío extremos, apoyo a sectores económicos marginados, uso eficiente de la energía, promoción del uso de electrodomésticos como estufas eléctricas, promover el uso de energías renovables, dar respuesta a la demanda, entre otros.

MI mide y registra el consumo de dispositivos/cargas en el hogar, así como la energía producida por los DER. Esto genera transacciones de energía de dos tipos: consumo (T_c) y producción (T_p). La información resultante se registra en la cadena de bloques para salvaguardar las lecturas. Además, las lecturas de T_c y T_p pueden asociarse con esquemas de compra/venta si se trata de consumir y producir electricidad (T_c -> T_b *y* T_p -> T_s).

En general, en sistemas balanceados como una microrred, habría una diferencia entre el consumo y la producción de energía. Si no hay producción de electricidad o intermitencia en la generación, se puede utilizar la generación de la empresa eléctrica. En cambio, cuando existe un excedente generado por los prosumidores, estos pueden vender la energía excedente siempre que cumpla con los criterios de calidad energética y los mecanismos de control derivados de las señales económicas. En el caso de que existan sistemas de almacenamiento, la energía se puede almacenar; de lo contrario, tendrá que inyectarse en la red eléctrica o desperdiciarse según las especificaciones acordadas del contrato inteligente.

De manera general, se conceptualiza una cadena de bloques privada ya que la empresa de suministro eléctrico debe ser la base del funcionamiento de la red eléctrica. La incorporación de nuevos usuarios debe estar controlada por una entidad reguladora. Aún así, también debe existir la flexibilidad necesaria para que todos los usuarios de cualquier tipo puedan participar en el mercado energético de forma clara y sencilla.

La Figura **3-25** muestra la interacción general de la cadena de bloques multinivel propuesta para TE. Todos los nodos de cada nivel verifican su consumo eléctrico utilizando los algoritmos de consenso de PoEf. La salida de PoEf expresó el costo final en cada período considerando los incentivos del modelo TE.

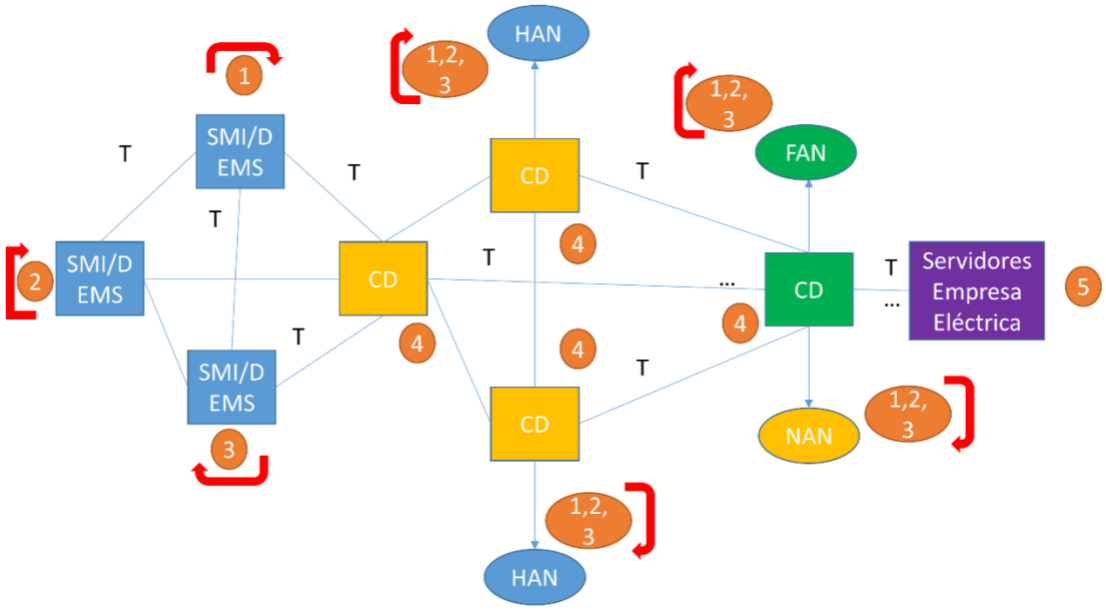

Figura 3-25 *Energía transactiva en un blockchain multi-nivel.*

La Figura **3-26** muestra el flujo principal del modelo propuesto y el **Algoritmo 5** describe el algoritmo de consenso para TES en detalle.

Para mejorar la comprensión del modelo propuesto, a continuación, se describen algunos escenarios y condiciones para comprender mejor el proceso.

Consideramos una tarifa plana de $1 MXN/kWh para el costo de consumo/producción/ingresos. Consideramos un descuento de Recompensas del 1% cada uno. Los otros parámetros son los indicados por defecto en el algoritmo de 1%.

Escenario 1. Consumidor con mejor desempeño en el vecindario (CD1) en el último período. Considerando un consumo total de 1kWh, no hubo producción por lo que los Costos = 0 - 1kWh * ($ 1/kWh) = - $1. El costo final = -1 + Recompensas - 0 (no hubo penalizaciones). La única recompensa fue R_a equivalente al costo * 1%, debido al costo final = -1 + (0.01) = $ -0.99, el consumidor debe pagar 99 centavos.

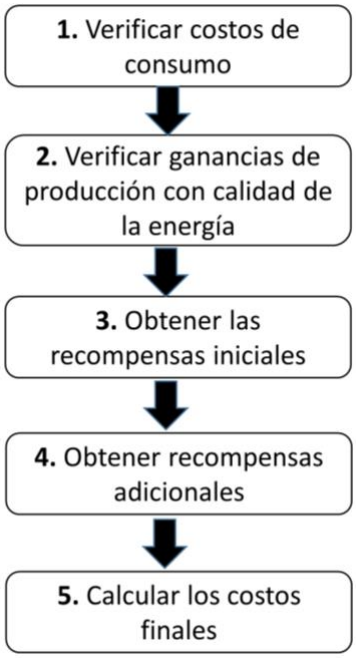

Figura 3-26 *Flujo principal del TES propuesto.*

Algoritmo 5 *Prueba de Eficiencia Versión 3*

Entrada: Un conjunto de transacciones de energía T_b / T_c, tiempo t (predeterminado 15 minutos, dependiendo del período de facturación de AMI), Criterios de calidad de energía (voltaje predeterminado +/- 5% valor nominal de 127 voltios, frecuencia de 60 Hz +/- 0.1, porcentaje de Calidad de la Energía (PQ) de producción aceptable)

1. Los nodos de la red registran sus lecturas de consumo/producción de energía. En el caso de equipos intermedios como concentradores de datos, los datos se registran desde los nodos de concentración. Los datos de los clientes se almacenan en los servidores de la compañía eléctrica. Se elabora un esquema de consumo-producción para determinar el consumo neto (ver Ecuación 3).

$$Costos = ganancias\ producción\ kWh - gasto\ de\ consumo\ kWh \quad (3)$$

Ecuación 3 Costos netos

2. En el caso de mayor producción de energía eléctrica, el MI debe verificar si se cumplen los criterios establecidos de calidad de la energía eléctrica (por defecto y por simplicidad del modelo y derivados de las características del medidor se consideran variables simples eventos simples con *swag* y *swell*). Así, la calidad de la energía se determina considerando un valor mínimo aceptable del 90%. Si la calidad de la energía es inferior al 90%, se descarta el registro de datos correspondiente. Además, se emiten multas de producción (P_p) en caso de falta de producción de energía y baja calidad, por ejemplo, un valor mínimo aceptado del 95%. El valor de *Pp* está relacionado con un porcentaje mínimo de calidad de energía establecido a priori, por ejemplo, la energía entre 90% y 95% con un T_{pe} de penalización de % tiempo y % por defecto del 10% del *t* total, producirá un descuento de P_p de 10% de los ingresos de producción cada 10% del tiempo.

3. Si los usuarios finales fueron más eficientes en comparación con el último período, al usuario se le asigna una recompensa inicial (*Ri*). Además, se otorga una recompensa adicional (R_e) si el nodo corresponde al nodo con la mejor eficiencia en el vecindario; requiere evaluar la eficiencia de todos los nodos. Se pueden otorgar recompensas adicionales (R_a) en función de condiciones operativas adicionales, como la ubicación geográfica, por ejemplo, la ciudad más eficiente.

4. Los dispositivos intermedios, como los CD, evalúan el rendimiento general de los nodos. Los dispositivos intermedios también determinan anomalías probables en el consumo producción de energía que pueden considerarse robo y/o fraude energético. Se podría considerar un esquema de recompensa (*Rtf*) para recompensar aquellas áreas donde no hay anomalías de este tipo. Este esquema se puede extender a otras funcionalidades, como el pronóstico de la demanda en tiempo real o los esquemas de respuesta a la demanda.

5. Finalmente, el cálculo del consumo neto derivado se muestra en Ecuación 4:

$$Costos\ Finales = Costoss + Suma\ Recompensas\ (R_{tf}, R_a, R_i, R_e) - Penalidades\ (P_p) \quad (4)$$

Ecuación 4 Costos Finales

Si el costo final es positivo es un ingreso para los prosumidores; de lo contrario, es un costo a pagar del prosumidor a la empresa de servicios públicos.

Salida: los costos finales de cada nodo (MI) en cada período.

Escenario 2. Consumidor con mejor desempeño en el último período. Considerando un consumo total de 1kWh, el Costo = $ -1. La recompensa es R_i porque este nodo tiene un mejor rendimiento en comparación con la facturación equivalente del último período, debido a los costos finales = -1 + (1 * 1%) = $ -0,99.

Escenario 3. Prosumidor con más consumo que producción con mejor desempeño en la ciudad. Considerando un consumo de 1kWh y una producción de 3kWh. El costo = 3kWh * ($ 1kWh) - 1kWh * ($ 1kWh) = $ 2. La recompensa en este caso es *Ra* y el costo final = $ 2 + (2 * 1%) = $ 2.02 que es una cantidad favorable para el usuario final.

Escenario 4. Prosumidor con más producción, pero mala calidad de energía (93%) durante dos minutos. Considerando el consumo de 1kWh y la producción de 2kWh, el costo = (2kWh * $ 1 / kWh) + (1kWh * $ 1 / kWh) = $ 1. El costo final = $ 1 +0 (porque no hubo recompensas) - Penalizaciones. Las Penalizaciones *Pp* = $ 1 * (2 * 10%) = $ 0.20, debido a los costos finales = $ 1 - $ 0.20 = $ 0.80.

Escenario 5. Consumidor con mejor desempeño en el vecindario en el último período y sin anomalías. Considerando un consumo de 1kWh, el costo = - $ 1. Las recompensas son R_i y R_{tf}, las recompensas son 1% + 1% = 2%. El costo final = - $ 1 + (1 * 2%) = - $ 0,98.

Además, el modelo TE propuesto incluye un contrato inteligente ligero para implementar el mecanismo de control. Por ejemplo, el Algoritmo 6 muestra un ejemplo de un contrato inteligente muy simple. En este caso, el contrato inteligente indica las acciones a realizar si un prosumidor quiere vender su excedente de energía y consumir por parte del proveedor. La línea 1 indica el nombre del contrato inteligente. La línea 2 indica la validez. La línea 3 indica que, si la calidad de la energía es superior al 90%, la consumirá el usuario final. La línea 4 indica si el precio de producción es mayor o igual a $1 que vende el usuario, en otro caso (línea 5) el usuario no vende y almacena la energía (el prosumidor debe tener baterías de almacenamiento).

Algoritmo 6 *Ejemplo de CI en la plataforma TES propuesta*

1. NAME: Sell_1

2. TIME: 2021/02/01 00:00:00 – 2021/02/28 23:59:59

3. IF power_quality > 90 THEN CONSUME

4. IF price >= $1 THEN SELL

5. ELSE STORE.

Capítulo 4 Resultados y validación de la solución propuesta

En este capítulo se muestran los resultados obtenidos al ejecutar la arquitectura propuesta en un entorno controlado. Para la evaluación de la propuesta se consideran cuatro casos bajo estudio: arquitectura de cadena de bloques, algoritmo de consenso PoEf versión 1, plataforma analítica de datos (PoEf versión 2) y prueba a la plataforma TES (PoEF versión 3).

4.1. Caso 1: Arquitectura de cadena de bloques multinivel para la protección de datos

La implementación de la arquitectura propuesta se centra en los niveles NAN y FAN/WAN de AMI. Los autores implementaron un SMI con cuatro SM y dos CD. Cada red NAN tiene dos MI. La Figura **4-1** muestra la arquitectura de cadena de bloques utilizada para las pruebas. Tenga en cuenta que los dispositivos de las cuatro HAN son los mismos.

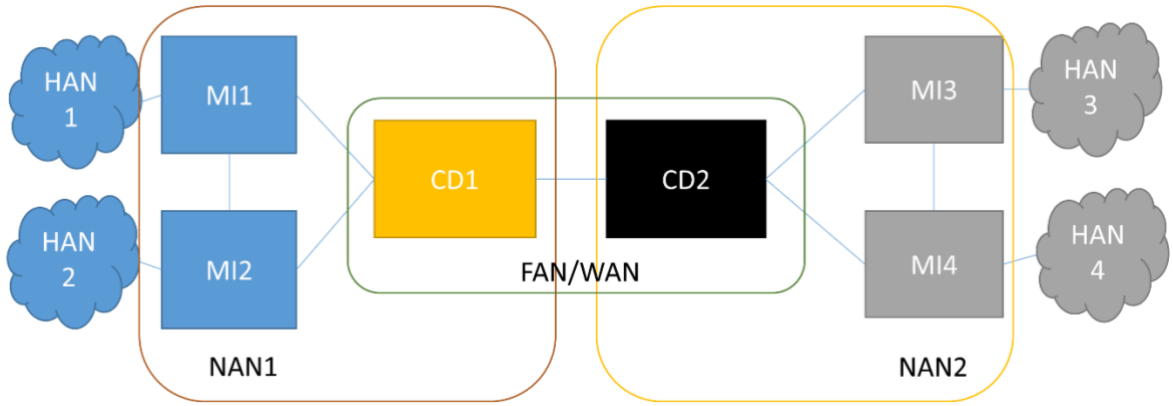

Figura 4-1 *La arquitectura implementada para las pruebas.*

La arquitectura de hardware elegida para el MI es una Raspberry Pi Model 3b con la tarjeta de energía Smart Pi Sensor [106]. El hardware para CD es una PC con 4GB en RAM, un disco duro de 1TB y microprocesador Intel core i5 a 3.8GHz conectado a una red FastEthernet mediante cableado UTP-Cat6. La selección de hardware se eligió basándose en pruebas previas que determinan la mejor SBC para un MI.

En la Figura **4-2**, se muestra el MI conformado por la integración del SBC Raspberry Pi y la tarjeta de energía SmartPi. En la Figura **4-3**, se muestra un ejemplo del software de medición modificado.

El sistema de Blockchain se ha implementado en lenguaje Python utilizando PostgreSQL 8.4 en MI y CD. El algoritmo hash utilizado es SHA-256. El contenido de la transacción está cifrado con AES-128 y RSA de 1024 bits se usa para las firmas en PKI. La Figura **4-4** muestra el diagrama de bloques de la implementación de la cadena de bloques en NAN.

Figura 4-2 *Arquitectura de hardware del MI.*

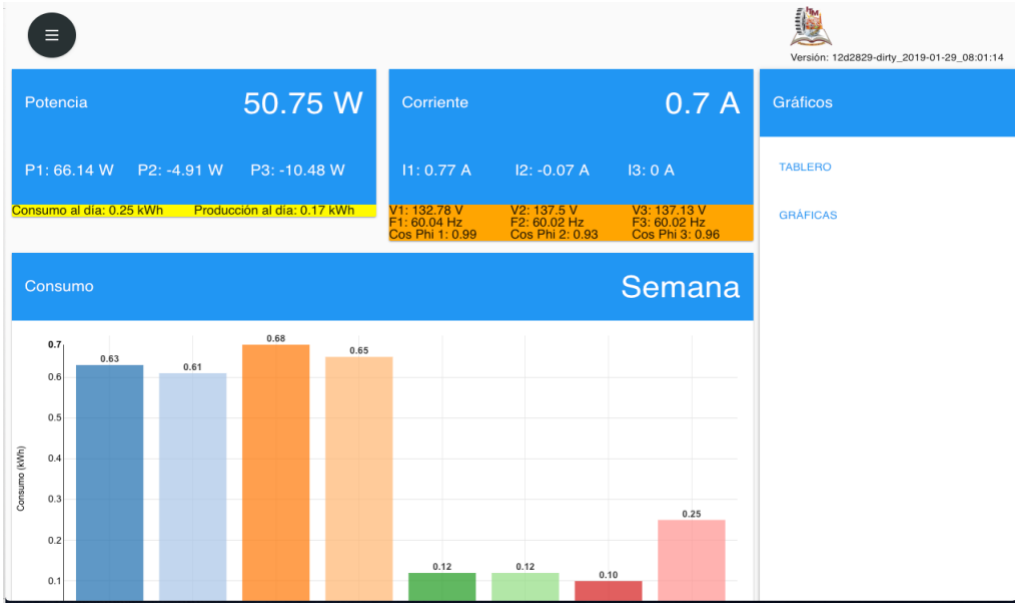

Figura 4-3 *Captura de pantallas del portal de medición modificado.*

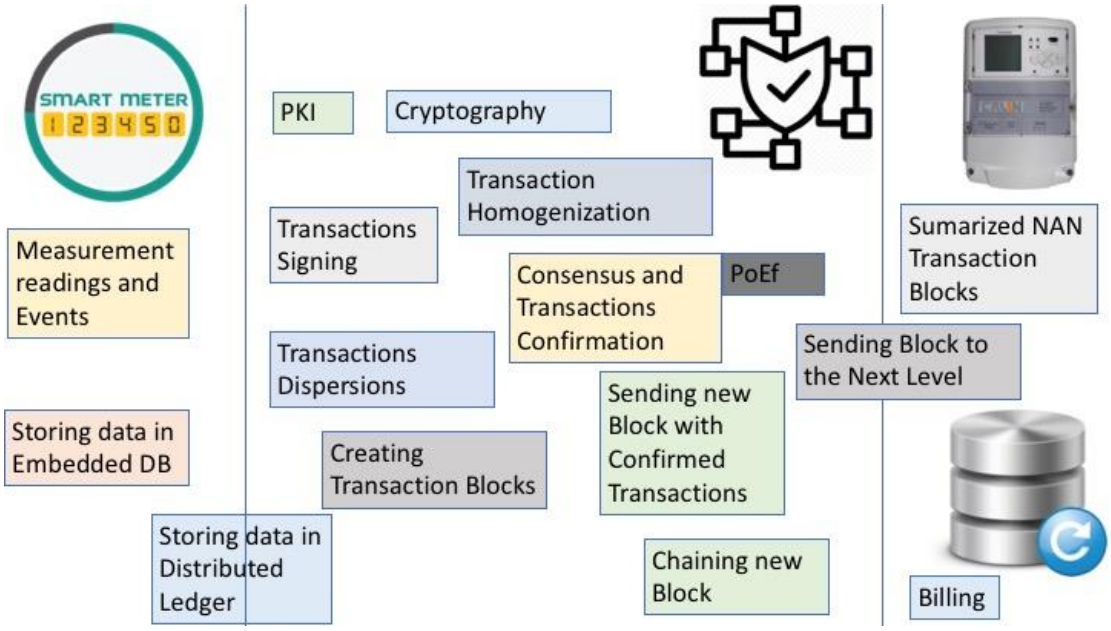

Figura 4-4 *Diagrama de bloques de la implementación de Blockchain en NAN.*

Nótese que la parte central son los módulos básicos y se implementan dentro del MI. En el lado derecho, se muestran el CD y el Servidor Head-end en el centro de datos.

Además, la arquitectura se probó en un modelo CD Texas Instruments TMDSDC3359 y en un MI Texas Instrument EVM430-F6779 utilizando la biblioteca de energía y procesando datos en una placa Raspberry Pi.

Para MI legados, es necesario agregar una placa de módulo de expansión para expandir la memoria RAM y la tarjeta SD para ejecutar el sistema operativo Linux embebido con Python y BD embebidas.

En esta sección, se muestra cómo la propuesta arquitectónica responde a algunos problemas de ciberseguridad en SMI. En primer lugar, los MI y los CD están reforzados en su sistema operativo Linux y servicios de Internet como Servidor Web de forma segura. Además, se utilizó un servidor de seguridad de host para las conexiones entrantes y salientes. Las comunicaciones utilizaron una VPN en cada capa de la cadena de bloques. De antemano, se usaron algunas herramientas de prueba de vulnerabilidades para verificar la ciberseguridad de todos los nodos.

1) Problemas generales de ciberseguridad de SMI

En general, las cadenas de bloques garantizan la ciberseguridad en diversos campos como Confidencialidad, Integridad, Disponibilidad, privacidad, entre otros. Para probar la manipulación de datos, se modificó en el MI2 una transacción que corrompe algunas lecturas. Todos los nodos, incluidos los coordinadores, pudieron verificar la manipulación de datos y evitar la transacción alterada.

En relación con la privacidad de los datos, en el libro mayor solo se almacenan el ID de los nodos: EI, DER, MI y CD. Por lo tanto, la información es pseudoanónima y es tan segura como cualquier cadena de bloques. Por confidencialidad, todos los nodos deben estar registrados en su coordinador y utilizar la infraestructura PKI para la firma de transacciones. Solo las claves públicas/privadas correctas pueden acceder a la información. La disponibilidad de los datos se probó a través de un ataque DoS realizado nuevamente en los nodos de la cadena de bloques. Se comprobó que cuando al menos un nodo está disponible, los datos de la cadena de bloques podrían restaurarse.

Para probar la inyección de datos falsos, los autores diseñan un escenario con ataques de precios en el nivel NAN de la cadena de bloques como se muestra en la Figura **4-5**. La empresa eléctrica envía un nuevo precio a la cadena de bloques (paso 1) y el precio se almacena en cada nivel (paso 2 al 4), por lo tanto, para manipular un precio de señal es necesario manipular todos los bloques de cada capa (paso 5). Los nodos siempre comparan su precio con sus coordinadores y descartan precios falsos.

Tenga en cuenta que la señal de precio se almacena en cada nivel de la cadena de bloques, para manipularla; es necesario modificar todos los bloques de la cadena de bloques. De manera general, la propuesta arquitectónica protege los datos de medición inteligente de manera adecuada.

2) Problemas generales de ciberseguridad de Blockchain

Para probar un ataque MitM, se utilizó un escenario simple en el que un nodo malicioso en el nivel NAN de blockchain quiere escuchar mensajes no autorizados. El nodo malicioso no puede escuchar ni escribir ninguna transacción debido a que no tiene las credenciales correctas para ingresar a la red de la cadena de bloques.

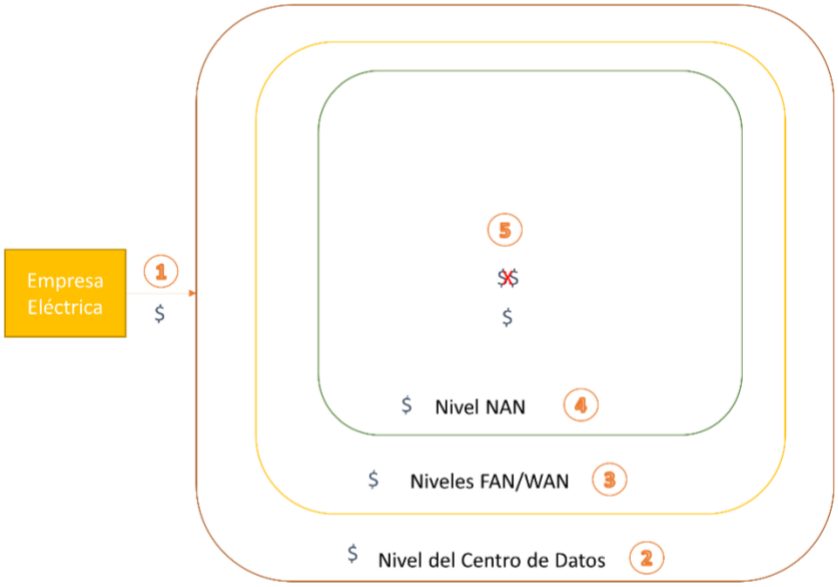

Figura 4-5 *Escenario de ataque de precio falso.*

El ataque del 51% es un problema grave de ciberseguridad en cadenas de bloques. El algoritmo de consenso propuesto funciona con un consenso de mayoría simple y podría ser vulnerable a este tipo de ataque. Para mitigar este ataque, la arquitectura propuesta ha implementado un sistema de alarmas para reportar transacciones de consumo/producción anormales. Estas alertas deben ser verificadas y analizadas para un mejor funcionamiento del sistema.

3) Problemas de ciberseguridad de la propuesta arquitectónica

El rol de coordinador de nodo es la parte más vulnerable de la arquitectura propuesta debido a su naturaleza centralizada. Por este motivo, es necesario saber cómo se detecta una falla de un nodo coordinador. Las fallas en los nodos coordinadores se detectan si la validación de las transacciones no ocurre correctamente. Todas las transacciones son confirmadas por la mayoría de nodos y el coordinador.

Para probar la ciberseguridad en los nodos coordinadores, los autores propusieron un escenario en la cadena de bloques de nivel FAN/WAN donde el coordinador está atacando usando DoS. Los resultados obtenidos muestran que el rol de coordinador puede pasar al segundo coordinador sin problemas solo con un retraso en la confirmación de las transacciones.

4) Pruebas de rendimiento

Respecto a los gastos generales, lo más visible está relacionado con el espacio en disco. Un MI normal tiene un promedio de 100 bytes por transacción cada 15 minutos. Una transacción con blockchain de varios niveles en el nivel NAN implica 375 bytes por transacción. Esto es 3 veces más grande.

La sobrecarga en el procesamiento no es relevante debido a que el tiempo promedio en el algoritmo PoEf se redondea a 1 minuto en NAN y 1.5 minutos en FAN/WAN y el tiempo para los informes de AMI es de 15 minutos.

Sobre la escalabilidad, la arquitectura propuesta podría incrementarse utilizando más nodos. Los autores han comprobado con la simulación de procesos que más de 2,000 nodos MI (una cantidad común en AMI para cada CD) podrían funcionar en el nivel NAN sin problemas de rendimiento.

5) Probando la ciberseguridad usando Gemelos Digitales

Recientemente ha surgido el concepto de Gemelos Digitales (DT, por sus siglas en inglés) que permite la interacción entre objetos físicos y virtuales, considerando un objeto virtual como una réplica del objeto físico permitiendo que ambos interactúen como si fuera uno solo. DT trae enormes ventajas ya que el mundo físico interactúa de la misma forma con el mundo virtual, alterando cualquier cambio en la realidad de los dos mundos [107].

Se desarrolló un marco de trabajo para DT compuesto principalmente por un controlador DT. El DT Framework Controller (DTFC) se encarga de mapear objetos reales con su representación virtual, intercambiar valores entre DT, notificar eventos y alarmas entre todos los objetos y simular ciberamenazas y ataques. La Figura **4-6** muestra los casos de uso descritos anteriormente del DTFC.

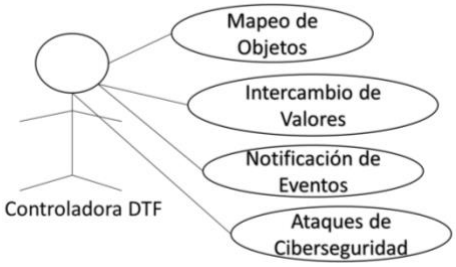

Figura 4-6 *Diagrama de Casos de Uso de un DT Framework Controller.*

Diseñar un DT de un SMI requiere del mapeo de objetos virtuales con objetos físicos en el MI. El MI utilizado está compuesto por una placa Raspberry Pi Modelo 3B + con el uso de una tarjeta de adquisición de datos de potencia SmartPi. El MI usa una distribución de Linux Raspbian, por lo que su mapeo es directo con el controlador DT. En el caso de los electrodomésticos, se ha agregado un módulo de comunicación WiFi y procesamiento de variables eléctricas a través de un microcontrolador Arduino y sensores de corriente y voltaje. Además, se han agregado un sensor de temperatura y un potenciómetro para controlar un aparato para encender o cambiar de velocidad. Para la implementación del sistema se modeló un DT de un MI, una plancha de 6 posiciones y una licuadora de 4 velocidades.

La arquitectura del DT propuesto se muestra en la Figura **4-7**. Se puede ver que hay seis objetos. Tres de los mundos físicos representados por la letra inicial P y que son la plancha, licuadora y un MI. Cada objeto físico tiene su componente virtual idéntico representado por la letra inicial V. Los electrodomésticos en el mundo físico tienen un Módulo de Procesamiento y Comunicaciones (MPC), que permite mapear con su contraparte tangible a través del controlador DT. El núcleo de la arquitectura es el controlador DT, que concentra información de objetos físicos con objetos virtuales para mapear cualquier cambio. La comunicación se realiza en ambos sentidos y con todos los objetos, tanto físicos como virtuales.

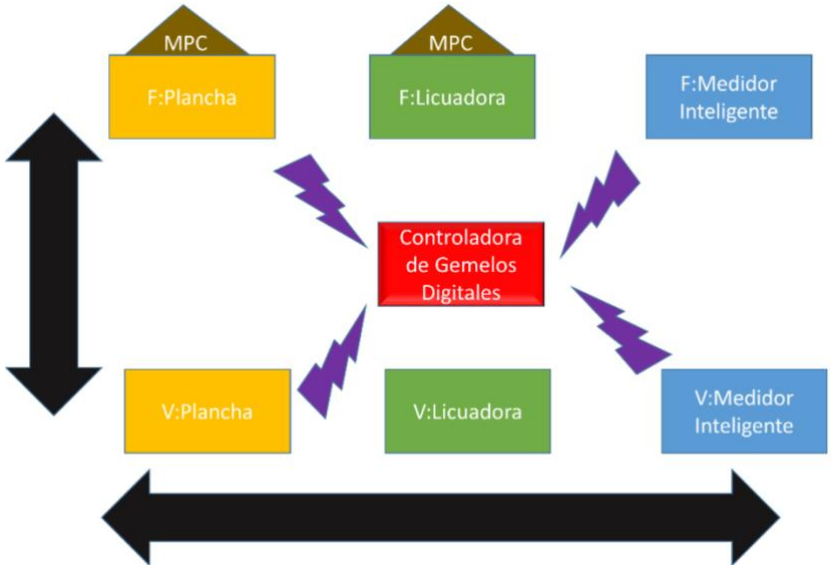

Figura 4-7 *Arquitectura de un prototipo DT para SMI en SH.*

Se utilizó el formato de Notación de Objetos de JavaScript (JSON, por sus siglas en inglés) para mapear los datos. Aquí hay un ejemplo de mapeo de los datos de DT en el MI:

```
{
   ID: 0x0001,
   Name: "Smart_Meter",
   On: 0,
   Voltage: 1,
   Current: 2,
   Power: 3,
   Consumption: 4
}
```

Existen datos de identificación particulares y valores que representan cada uno de los datos. En el caso de un MI, la posición 0 del potenciómetro indica que el dispositivo está apagado, mientras que las otras posiciones indican variables de energía eléctrica que se quiere monitorear. En el caso de la licuadora, los estados del potenciómetro indican las diferentes velocidades, mientras que en la plancha indican tipos de ropa para planchar. El calor de la plancha se monitorea con el sensor de temperatura.

Para cada objeto físico, es necesario un proceso de mapeo para obtener un objeto virtual. El objeto JSON representa un objeto virtual y el controlador DT puede agregarlo manualmente o descubrirlo.

La implementación del DT se realiza en python debido a su sencillez y alta portabilidad con otras plataformas. Cada objeto físico tiene configurada una dirección IP y se registra en el controlador mediante mapeo de datos. Una vez que se han producido los cambios, se muestran en la interfaz de DT y se reflejan en los objetos físicos y virtuales.

La comunicación entre objetos físicos es directa. No es necesaria una modificación en el sistema físico. En este caso, el SMI funciona con normalidad e interactúa con otro EI. La comunicación entre objetos virtuales se realiza directamente a través de la plataforma DT. El controlador DT se encarga de comunicar los cambios de los objetos virtuales a los físicos y viceversa. Además, el controlador DT siempre supervisa la interacción entre los objetos físicos y virtuales y refleja los cambios.

La plataforma DT puede detectar algunas amenazas cibernéticas, como ataque de sensor, ataque de nodo de suplantación, ataque de manipulación de hardware, ataque de manipulación de energía, rastreo, denegación de servicio distribuido (DDoS), fuga de datos confidenciales y tolerancia a fallas. Cada tipo de amenaza se describe a continuación y cómo la plataforma DT puede ayudar a probar la ciberseguridad en un HI.

Ataque de sensor

Cada dispositivo registrado en la plataforma debe registrar cada sensor. La plataforma DT registra los datos de los sensores de cada dispositivo en una base de datos histórica. La plataforma DT monitorea estos datos históricos y envía una alarma si el sensor tiene un comportamiento anómalo probable que pueda considerarse como un posible ataque.

Ataque de parodia (*spoof*)

Cada dispositivo registrado en la plataforma registra y toma una identificación única de la función de hardware. La plataforma DT monitorea esta identificación única de forma continua y evita un posible dispositivo de suplantación.

Ataque de manipulación de hardware

Cada dispositivo registrado en la plataforma debe verificar en su PCM un proceso de seguridad responsable de verificar todos los componentes de hardware si están conectados o desconectados.

Ataque de manipulación de energía

Similar al ataque de sensor, la plataforma DT monitorea el consumo histórico de cada dispositivo registrado. Si el consumo varía en un valor atípico, se envía una notificación al usuario.

Ataque de olfateo (*sniffing*)

La plataforma DT siempre monitorea la conexión de red de todos los dispositivos registrados, tanto físicos como virtuales. Cuando se detecta una nueva conexión, la plataforma DT registra la nueva conexión y notifica a los usuarios. La comunicación entre objetos físicos y virtuales se cifra mediante firmas RSA.

Ataque distribuido de denegación de servicio (DDoS)

La plataforma DT tiene un firewall integrado responsable de verificar las conexiones de red. Solo los dispositivos registrados, tanto físicos como virtuales, pueden conectar cada uno. La plataforma DT registra la frecuencia de comunicación de cada dispositivo y notifica a los usuarios del uso anormal.

Ataque sensible y de fuga de datos (SDL)

La plataforma DT solo permite que los dispositivos registrados y autorizados vean y exporten la información. La plataforma DT requiere otorgar permisos para acceder a datos sensibles.

Tolerancia a fallos

El cuello de botella en los sistemas centralizados es el proceso del servidor, en nuestro caso, el controlador DT. La plataforma DT puede conectarse con otros controladores DT como respaldo. Cuando la plataforma DT detecta una falla, si existe un controlador DT auxiliar, el controlador auxiliar se conmuta como un nuevo controlador DT. Los controladores DT auxiliares verifican la base de datos con toda la información actualizada.

Se desarrolló un escenario de ciberseguridad para probar aspectos de ciberseguridad en HI. El escenario de prueba está relacionado con la manipulación de datos de forma física y lógica. El escenario de prueba tiene en cuenta los diversos ataques y amenazas mencionados anteriormente en esta sección.

La Figura **4-8** muestra los diferentes ataques utilizados en el escenario de prueba de manipulación. Los lectores pueden observar que se prueban tanto los objetos físicos como los virtuales.

Ejecutamos el escenario de manipulación de datos 100 veces, obteniendo los resultados descritos en la Tabla **4-1**.

Se puede observar que la mayoría de los casos son 100% seguros. Solo los ataques de manipulación de energía y sensores tienen un porcentaje distinto del 100%. Estos ataques tienen un comportamiento no lineal debido a que los componentes se basan en sus registros históricos del uso de cada sensor/energía y es difícil detectar si un valor anormal podría considerarse como un ataque.

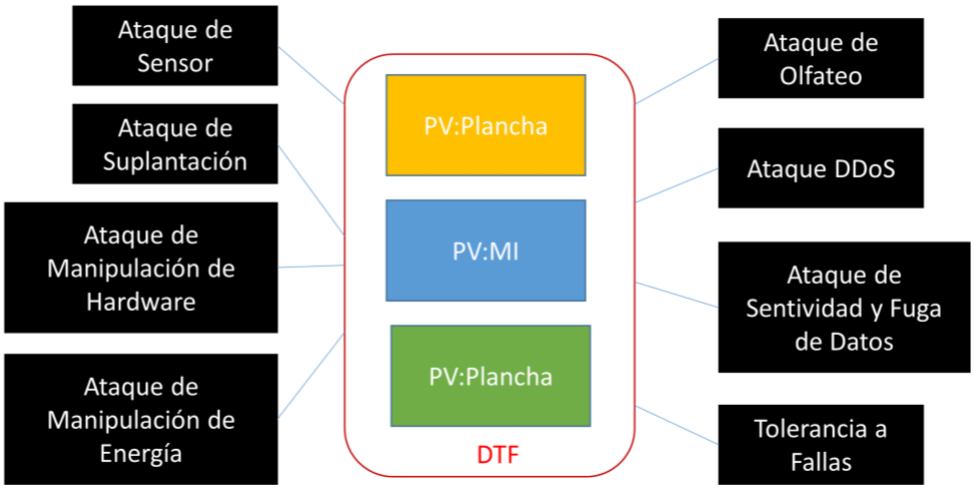

Figura 4-8 *Escenario de pruebas de manipulación.*

Tabla 4-1 *Resultados del escenario de manipulación.*

Ataque	**MI**	**Plancha**	**Licuadora**
Sensor	89	95	100
Parodia	100	100	100
Manipulación de Hardare	100	100	100
Manipulación de energía	93	96	100
Olfateo	100	100	100
DDoS	100	100	100
SDL	100	100	100
Tolerancia a fallos	100	100	100

4.2. Caso 2: Algoritmo de Consenso PoEf versión 1

Las pruebas se realizaron en la red NAN del SMI para leer el consumo de energía y la producción obteniendo una base de datos de 1,382,400 registros de un experimento de 30 días. Las lecturas de SM fueron de 8 por minuto, esto con el objeto de tener màs cantidad de registros.

La Figura **4-9** muestra los resultados del entrenamiento del algoritmo para predecir el próximo valor en la transacción de energía de consumo/producción.

Tenga en cuenta que la línea azul son los datos históricos, mientras que la línea roja es la predicción usando los datos anteriores para el ajuste. El eje x representa 240 días (seis meses), mientras que el eje y representa el consumo/producción de datos expresados en kWh.

Los cuatro MI estaban conectados a los mismos electrodomésticos en el HAN una licuadora, un microondas, dos reproductores de DVD, dos TV Color (32" y 40"), una lavadora automática, una plancha de ropa, una computadora de escritorio y un refrigerador (18 a 22 pies^3). La Figura **4-10** muestra el consumo de los MI por día en el experimento de 30 días.

La cadena de bloques en el nivel NAN ha sido evaluado en el sistema durante 30 días con un tiempo de consenso de 15 minutos. Todas las transacciones se pueden verificar. A continuación, se comentan los resultados obtenidos.

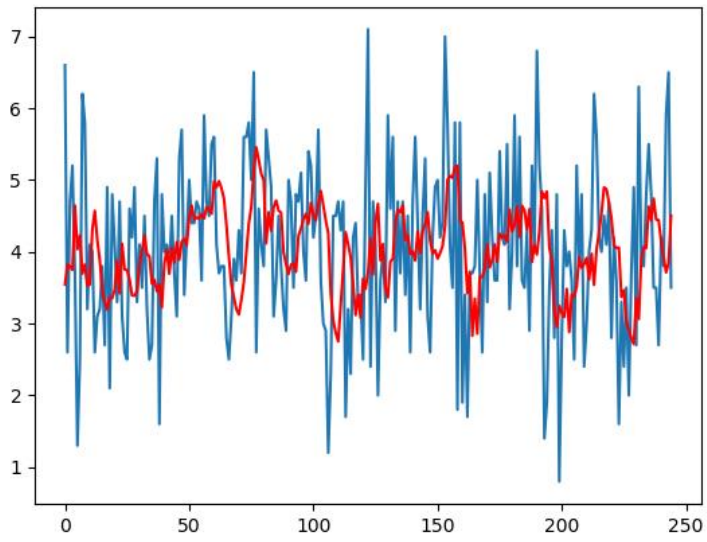

Figura 4-9 *La predicción de energía de las transacciones usando PoEf versión 2.*

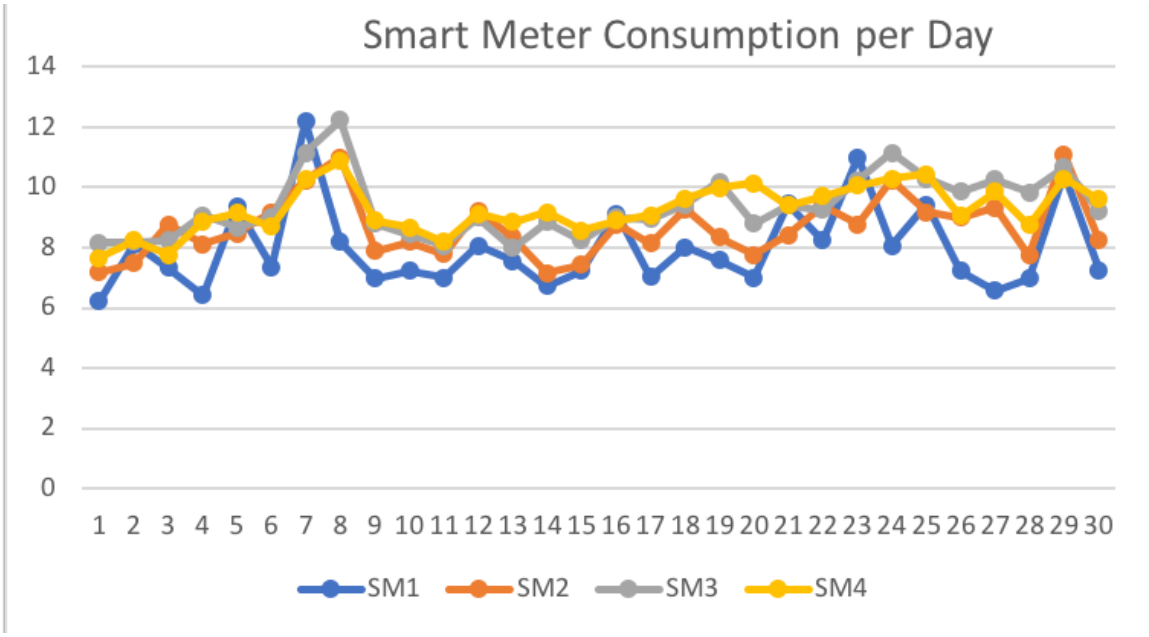

Figura 4-10 *Consumo de medidores inteligentes por día. El eje x representa los días y el eje y representa el consumo por día en kW/h.*

Hubo 96 períodos de tiempo de consenso de blockchain por día y 2,880 por mes. Cada período de consenso tuvo cuatro transacciones. El tamaño medio de cada transacción fue de 392 bytes. El tamaño total de la cadena de bloques para el experimento de 30 días fue de 1.08 MB.

En el nivel NAN se utilizó el algoritmo PoEf versión 1 extendida, mientras que en el nivel FAN/WAN se implementó la versión 1 básica con un período de 10 minutos para el consenso. Hubo 144 períodos por día y el tamaño total de esta cadena de bloques fue de 1,544 MB (el tamaño promedio fue transacción de 375 bytes) en el nivel FAN/WAN.

En México, las tarifas eléctricas residenciales son sencillas. Las tarifas para el período agosto 2018 se calculan de la siguiente manera [100]: los primeros 75 kWh, son $ 0.799 MXN (pesos mexicanos. 1 USD es aprox. 20MXN) los siguientes 65 KwH son $ 0.964 y 2.824 por el exceso de consumo.

La Tabla **4-2** muestra el consumo, la facturación, el MSE y el porcentaje de transacciones de recompensa en los experimentos en cadenas de bloques NAN.

La

Tabla **4-3** muestra los resultados de la aplicación de la versión 1 de PoEf en la cadena de bloques en el nivel FAN/WAN. Tenga en cuenta que cada blockchain en el nivel FAN/WAN incluye el consumo de su CD. Además, el porcentaje de transacciones recompensadas considera todas las transacciones distribuidas en las 2 redes de cadenas de bloques NAN.

Tabla 4-2 *Transacciones de consumo de medidores inteligentes, facturación y recompensas en cadenas de bloques NAN.*

MI	Consumo kWh	Facturación normal (MXN)	Transacciones recompensadas por PoEf	MSE
1	239.37	431.44	16.66%	0.77
2	260.09	489.95	14.33%	0.98
3	280.65	548.02	6.66%	1.73
4	278.22	541.15	10.2%	1.36

Tabla 4-3 *Consumo de concentradores de datos, facturación y transacciones recompensadas en blockchain.*

CD	Consumo kWh	Facturación Normal (MXN)	Transacciones recompensadas por PoEf
1	503.87	921.39	59.34%
2	563.29	1089.17	40.66%

Los resultados muestran que el MI con mayor eficiencia energética puede obtener una mejor recompensa de facturación. Además, si una NAN es más eficiente que otra, puede obtener recompensas adicionales para todos los MI de su red.

4.3. Caso 3: Plataforma de analítica de datos (PoEf versión 2)

Las pruebas se realizaron en los niveles HAN y NAN (Partes 1 y 2 de la arquitectura propuesta). El hardware y la comunicación de datos utilizados para probar la metodología constaba de tres componentes principales:

- MI: 4 Raspberry Pi modelo 3B + con placa SmartPi.
- CD: 1 Latte Panda Alpha con 8 MB en RAM y Sistema Operativo Linux.
- Medios de comunicación: WiFi, Gigabit Ethernet y PLC a 54 Mbps.

a) Resultados de probar la metodología de pronóstico de consumo

La medición del consumo y la producción de energía a una velocidad de 1 muestra por minuto da como resultado una base de datos de 43,200 registros en el MI. La Tabla **4-4** muestra un ejemplo de registros de base de datos obtenidos para consumo y producción de energía de un MI.

El CD analiza los datos de los 4 MI en diferentes ventanas de tiempo: día, semana, mes y año. El CD calcula un nuevo modelo basado en datos anteriores de un mes y año y lo envía de vuelta al MI correspondiente. Dado que el CD obtiene datos de 4 MI, la BD resultante contiene 172,800 registros. La

Tabla **4-5** muestra la base de datos en CD usando una BD SQLite.

Tabla 4-4 *Base de datos del medidor inteligente para grabar registros de Consumo y Producción.*

Marca de tiempo	Consumo (kWh)	Producción (kWh)
2019/04/11 10:00:00	0.109	0
2019/04/11 10:01:00	0.083	0
2019/05/10 09:59:00	0.116	0.054

Tabla 4-5 *Base de datos del CD parar grabación del consumo y producción de energía en NAN.*

Marca de Tiempo	Número de Identificación del Medidor (SM_ID)	Consumo (kWh)	Producción (kWh)
2019/04/11 10:00:00	1	0.109	0
2019/04/11 10:00:05	2	0.097	0.114
2019/04/11 10:00:09	3	0.201	0
2019/04/11 10:00:13	4	0.145	0

La Figura **4-11** muestra las lecturas del consumo de energía de un SM. La curva de consumo tiene algunos picos altos algunos días, otros días no tiene consumo y otros días tiene un consumo constante. El eje x representa los días de un mes y el eje y representa el consumo de energía en kWh por día.

La Figura **4-12** muestra las lecturas de producción de energía usando un panel fotovoltaico. Nuevamente, el MI registra lecturas de producción algunos días, la producción es cero en otros días. El eje x representa los días de un mes y el eje y representa la producción de energía en kWh por día. Los valores negativos indican que se produce energía; los valores de energía positivos indican que se consume energía.

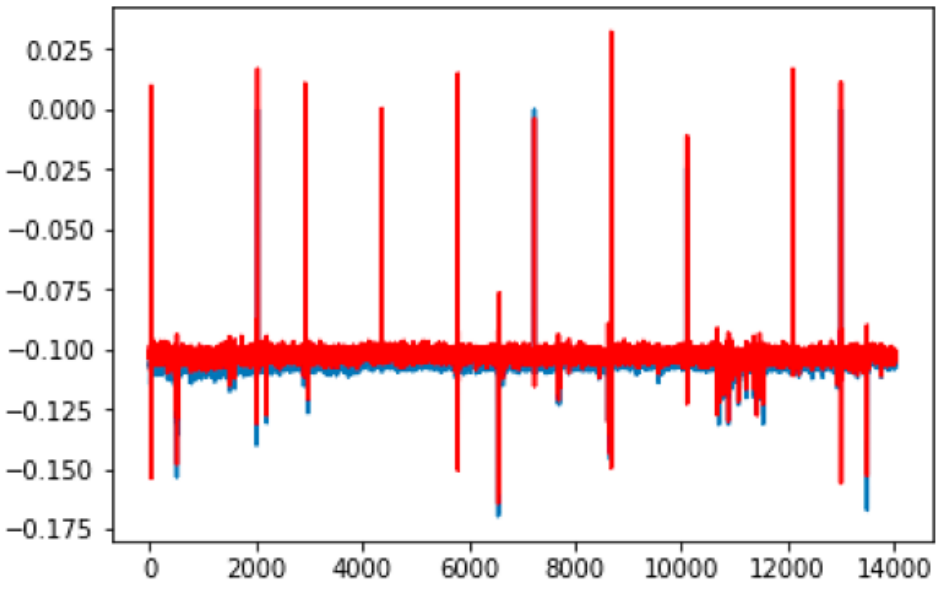

Figura 4-11 *Predicción de producción de energía en medidor #2.*

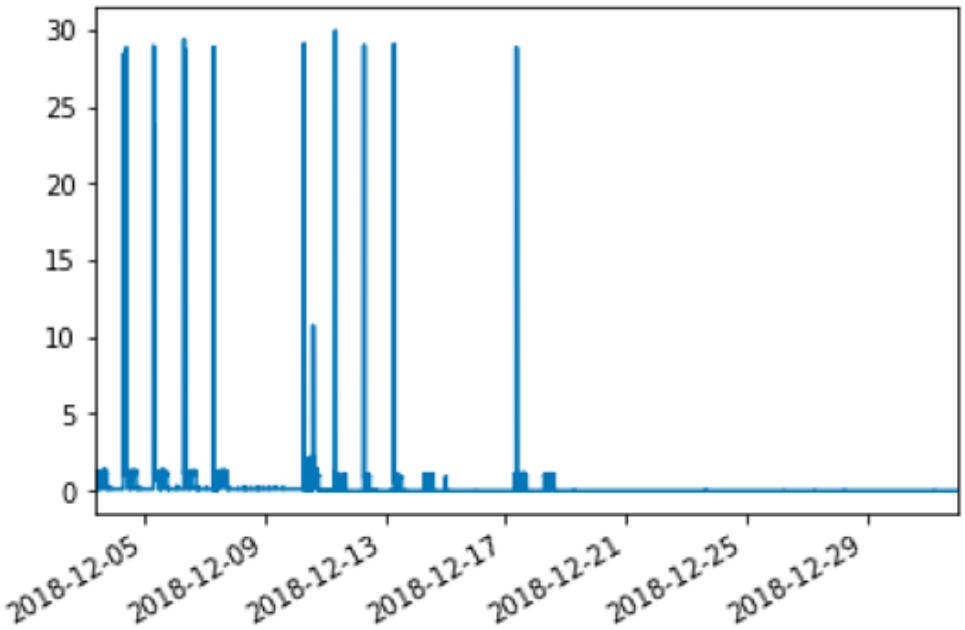

Figura 4-12 *Lectura de consume de energía del medidor inteligente #1.*

Además, en la Figura **4-13** se muestra la previsión del consumo de energía calculada en el MI2). MI2 tiene lecturas de producción y consumo. El eje x representa el número de lecturas de consumo / producción días de un mes y el eje y representa el consumo de energía en kWh por día. Se ajusta la escala en el eje y.

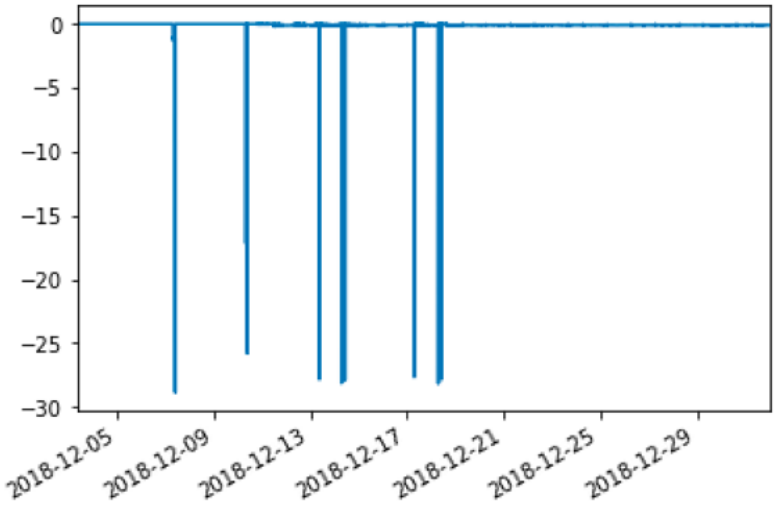

Figura 4-13 *Lecturas de producción de energía del medidor inteligente #2.*

Los resultados muestran un MSE de 0.019 en lecturas de consumo y 0.001 en lecturas de producción. Los resultados experimentales muestran que la arquitectura propuesta puede proporcionar un consumo/producción de energía cercano utilizando el enfoque de series de tiempo.

La metodología funciona de la siguiente manera: cuando se obtienen nuevos datos, se compara con los datos predichos y posteriormente se compara con los datos observados calculando la desviación del error y la tasa de aprendizaje mediante un proceso RL. En esta aplicación de análisis de datos, los estados son Al y los diferentes Au. Las acciones se predicen o se ajustan. Las recompensas son (1 ó -1) dependiendo de la función de valor que dan las métricas de error como MSE. El entorno y las políticas mapean la transición entre Al y diferentes Au de acuerdo con las capacidades del hardware y los Vf (s). Por último, la función de aprendizaje se obtiene comprobando Al(s) con Vf (s) mediante la observación. La Tabla **4-6** muestra los resultados de experimentar durante un período de 30 días usando 4 MI y 1 CD. La evaluación se probó 12 veces. Tenga en cuenta que Qi representa la tasa de aprendizaje donde i es el número de prueba: Q1 es la tasa de aprendizaje en el primer período y así sucesivamente. Los valores de Q se expresan en porcentajes.

Tabla 4-6 *Rangos de aprendizaje en la aplicación de análitica de datos en el pronóstico de consumo/producción.*

MI	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12
1	51.21	53.21	53.53	53.98	54.93	56.52	58.09	58.33	59.59	62.04	641.72	64.81
2	48.85	49.71	50.91	52.03	55.51	55.85	57.83	58.85	59.93	61.28	62.36	62.36
3	53.44	53.93	54.93	55.55	57.2	57.23	58.82	59.98	60.78	62.09	63.45	63.45
4	50.88	51.33	52.75	53.27	55.16	56.01	57.17	57.87	59.03	60.18	61.37	62.53

Los resultados obtenidos muestran que la arquitectura propuesta en esta aplicación analítica de datos puede aprender de manera efectiva debido a que el nuevo MSE con RL fue de 0.014 en consumo y 0.07 en producción.

b) Resultados de probar la metodología de predicción de calidad de la energía

La estructura de la BD del MI se muestra en la

Tabla **4-7**.

Tabla 4-7 *Base de datos SM para clasificar eventos de calidad de la energía.*

Marca de Tiempo	Voltaje (V)	Frecuencia (Hz)
2019/04/11 10:00:00	120.53	60
2019/04/11 10:00:01	127.29	60
2019/04/11 10:00:03	128.12	59.98

El clasificador utiliza un estado vectorial de tamaño 60 para evaluar los eventos ocurridos. Un estado vectorial con valores de voltaje y otro con valores de frecuencia se utilizan para registrar los eventos de calidad de energía. Cada evento tiene un número de identificación que representa la clase de identificación de cada categoría (ver Tabla **4-8**).

La Tabla **4-9** muestra un ejemplo de las primeras 7 posiciones en el vector de estado de valores de voltaje. Este ejemplo se clasifica como un evento de hundimiento temporal porque su frecuencia tiene cuatro segundos entre 0.8 y 0.9 por unidad (pu).

La Tabla **4-10** muestra los resultados de clasificación almacenados en el MI. La duración se expresa en segundos.

Las mediciones originales y los eventos de calidad de la energía que ocurrieron se envían al CD para su procesamiento. El CD genera un modelo para la red NAN que representa el estado de la red de distribución. La Tabla **4-11** muestra los resultados de la clasificación de eventos reportados para cada MI en el CD.

Durante un mes de experimentación, se registraron 5,417 eventos de calidad de energía. El evento más común fue un swag momentáneo. Los resultados completos se muestran en la Tabla **4-12**.

La Tabla **4-13** muestra el número de clasificaciones correctas e incorrectas en la clasificación de la calidad de la energía. Los resultados son una media de 30 experimentos en los 4 MI.

Tabla 4-8 *Tabla de IDs representando eventos de calidad de la energía.*

ID de clase	Descripción
0	No evento
1	Interrupción momentaria
2	Interrupción Temporal
3	Interrupción sostenida
4	Hundimiento momentáneo
5	Hundimiento Temporal
6	Bajo voltaje
7	Oleaje momentaneo
8	Oleaje Temporal
9	Sobrevoltaje
10	Variación de frecuencia corta
11	Variación de frecuencia media
12	Variación de frecuencia larga

Tabla 4-9 *Vector de estado representando eventos de calidad de la energía.*

0	0	1	1	1	1	0…0

Tabla 4-10 *Base de datos de clases en SM.*

Marca de tiempo	ID_clase	Duración
2019/04/11 10:01:00	5	4
…	…	…
2019/04/11 10:14:00	2	11

Tabla 4-11 *Base de datos en el CD con una clasificaciín de eventos de calidad de la energía en HAN.*

Marca de tiempo	**SM_ID**	**ID_clase**	**Duración**
2019/04/11 10:01:00	1	5	4
2009/04/11 10:05:00	2	4	3
2019/04/11 10:14:00	4	2	11

Tabla 4-12 *Clasificación de eventos de calidad de la energía en CD.*

MIs	**Eventos**											
	C1	**C2**	**C3**	**C4**	**C5**	**C6**	**C7**	**C8**	**C9**	**C10**	**C11**	**C12**
MI1	5	0	0	253	203	21	753	147	53	7	1	0
MI2	19	2	3	288	181	29	299	133	68	4	3	1
MI3	11	1	2	268	173	37	627	214	51	5	2	0
MI4	13	1	0	247	164	27	802	218	73	7	5	1

Subtotal	43	4	5	1056	721	114	2481	712	245	23	11	2

La metodología es similar a la descrita en el apartado a) con las siguientes diferencias:

Las acciones se clasifican o ajustan. Las recompensas son dos valores (1 ó -1) dependiendo de la función de valor que dan las métricas de error como una matriz de confusión (las clasificaciones correctas dan 1 recompensa, las clasificaciones incorrectas dan -1).

Tabla 4-13 *Matriz de confusión de clasificación eventos de calidad de la energía.*

		Predicción	
		Positivos	**Negativos**
Observación	**Positivos**	2124	662
	Negativos	661	1970

La Tabla **4-14** muestra los resultados experimentando durante un período de 30 días utilizando 4 MI y 1 CD, de manera similar al apartado a).

Los resultados obtenidos muestran que la arquitectura propuesta en esta aplicación analítica de datos puede aprender de manera efectiva debido a que el proceso de clasificación tiene una puntuación de 90.53% de casos correctos y con RL se mejoró a 98.17%.

Tabla 4-14 *Tasas de aprendizaje en Clasificación de Eventos calidad de la energía.*

MI	**Q1**	**Q2**	**Q3**	**Q4**	**Q5**	**Q6**	**Q7**	**Q8**	**Q9**	**Q10**	**Q11**	**Q12**
1	92.79	93.07	94.18	95.43	96.26	96.67	97.09	97.64	97.92	98.34	98.89	99.31
2	96.8	96.99	97.28	97.96	98.35	98.74	99.32	99.51	99.71	99.71	99.71	99.71
3	79.3	80.88	84.54	86.13	87.92	90.15	91.23	91.88	93.39	94.32	95.11	95.18
4	93.26	94.74	95.51	95.89	96.53	97.75	97.88	98.01	98.2	98.4	98.46	98.46

c) Resultados de probar la metodología de Predicción de Robo de Energía

El modelo de datos se obtiene de la metodología de previsión del consumo de energía de prueba (

Tabla **4-4** y

Tabla **4-5** en MI y CD respectivamente). Además, se utilizan dos repositorios de datos más en MI y CD para almacenar las predicciones y calcular el porcentaje de la diferencia entre los datos de consumo/producción de energía como se muestra en las Tabla **4-15** y la Tabla **4-16**.

Tabla 4-15 *Base de datos del MI para registro de predicciones de Consumo y Producción.*

Marca de tiempo	Predicción de consumo (kWh)	Delta de consume (kWh)	Predicción de producción (kWh)	Delta de produccion (kWh)
2019/04/11 10:00:00	0.115	0.06	0	0
2019/05/11 10:01:00	0.080	-0.03	0	0
2019/05/11 22:03:00	0.099	+0.11	0.066	-0.07
2019/05/12 09:59:00	0.116	-0.04	0.054	0.05

Tabla 4-16 *Base de datos CD database para grabación de predicciones de consumo y producción en NAN.*

Marca de tiempo	SM_ID	Consumo predicho	Delta consumo	Predicción de producción	Delta de producción
2019/04/11 10:00:00	1	0.115	0.06	0	0

2019/04/11 10:00:05	2	0.094	-0.03	0.112	-0.02
2019/04/11 10:00:09	3	0.204	0.03	0	0
2019/04/11 10:00:13	4	0.149	0.04	0	0

La Tabla **4-17** muestra los resultados de la predicción del Robo de Energía en comparación con las observaciones. Los valores en las predicciones de consumo y producción se expresan en porcentajes indicando los datos correctos clasificados.

La Tabla **4-18** muestra el número general de clasificaciones correctas e incorrectas en la detección de ladrón de energía en consumo y producción de energía. Los resultados son una media de 30 experimentos en los 4 MI.

Tabla 4-17 *Resultados CD en aplicación analítica de datos para predicción de robo de energía.*

SM_ID	Consumo predicho	Predicción de producción
1	88.35	93.12
2	89.12	92.15
3	87.23	92.63
4	90.01	92.27

Tabla 4-18 *Matriz de confusion de detección de robo de energía.*

		Predicción	
		Positivos	**Negativos**
Observación	**Positivos**	19421	2009
	Negativos	2047	19723

La metodología es similar a la descrita en el apartado b) con los mismos parámetros en estados, acción, recompensas, función de valor.

La Tabla **4-19** muestra los resultados de la experimentación de 30 días usando 4 MI y 1 CD de manera similar a la sección a) y b).

Tabla 4-19 *Tasas de aprendizaje en Clasificación de Robo de Energía.*

MI	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12
1	87.23	87.65	87.87	88.07	88.29	88.73	88.99	90.12	90.43	90.61	90.735	90.735
2	87.11	87.33	87.67	87.91	88.13	88.44	88.69	88.95	90.12	90.24	90.39	90.635
3	88.13	88.22	88.37	88.51	88.68	88.81	89.11	89.27	89.43	89.93	89.93	89.93
4	90.17	90.23	90.31	90.47	90.63	90.77	90.88	90.94	91	91.05	91.09	91.14

Los resultados obtenidos muestran que la arquitectura propuesta en esta aplicación analítica de datos puede aprender de manera efectiva debido a que el proceso de detección de ladrones de energía tiene un puntaje general de producción/consumo de 88.16% de casos correctos y con RL se mejoró a 90.61%.

4.4. Caso 4: Probando la plataforma TES (PoEf versión 3)

El SM implementado utiliza una SBC Raspberry Pi Modelo 3B + con tarjeta de energía Smart Pi. La cadena de bloques, la plataforma de análisis de datos y el software TE se desarrollaron con Python y el software es portable para cada nivel de la arquitectura. El CD se implementó utilizando un SBC LattePanda Alpha con Linux como sistema operativo. El servidor utilizado como MDBS fue Linux Debian en HPE Proliant Server DL325 con 32 GB de RAM y 16 TB de almacenamiento.

El conjunto de datos utilizado fue la BD embebida de los MI, CD y Server utilizados en la prueba física. Se utilizaron tres CD para interconectar tres microrredes HAN de 3, 2 y 2 SM cada una. El CD3 estaba interconectado con el servidor de servicios públicos. En esta prueba, verificamos durante un período de un año el funcionamiento de la arquitectura SMI/TES.

Para probar y presentar los resultados, utilizamos un conjunto de datos reducido obtenido con permiso de CFE (CFE MDMS). El conjunto de datos contiene información de 4,238 MI que representan tres tarifas nacionales (1, 1D, 1F). Completamos el conjunto de datos con los mismos datos, pero faltan las otras tarifas y precios. El período del conjunto de datos fue de cuatro años correspondientes a marzo de 2016 a julio de 2020. Las transacciones de energía se registraron cada 15 minutos.

La Figura **4-14** y la Figura **4-15** muestran el porcentaje de transacciones de recompensa en verano y fuera de los veranos. Observe que el porcentaje en las tasas medias (1C y 1D) tiene el mejor porcentaje de transacciones de recompensas y aparentemente el porcentaje más bajo en el extremo, por lo que las mejores tasas son más frías o más calientes y los mejores ahorros están en la temperatura templada.

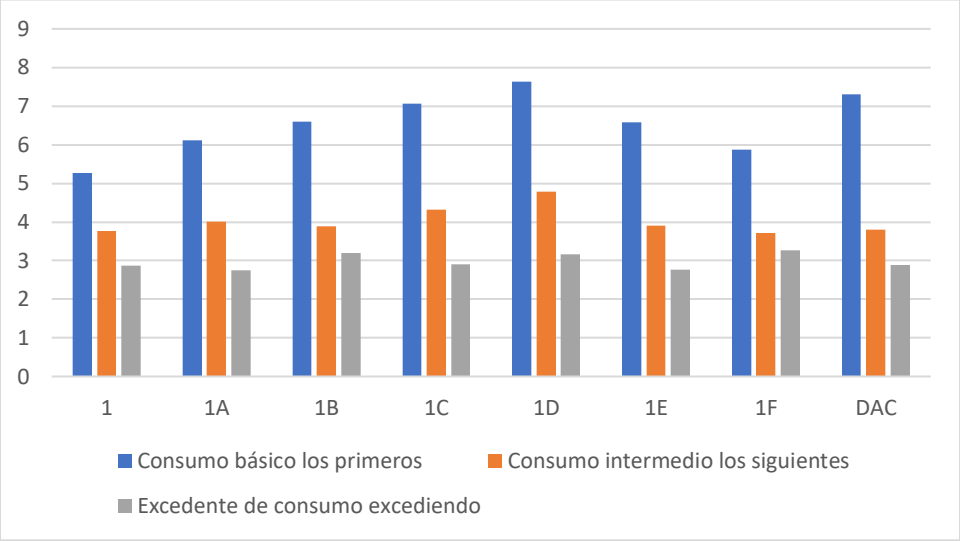

Figura 4-14 *Porcentaje de transacciones recompesadas fuera de verano.*

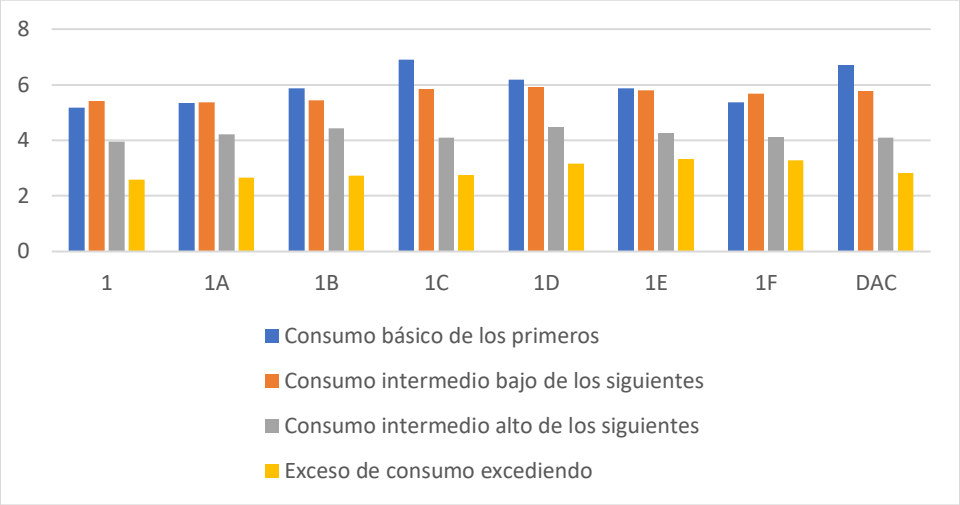

Figura 4-15 *Porcentaje de transacciones recompensadas en verano.*

Se consideró usar una tarifa plana en lugar de subsidios en la demanda (eliminó la estructura escalonada) y no considerar la temporada. La propuesta consideró solo la temperatura y el consumo (premiar el uso de producción de energía limpia). Si el prosumidor o participante del mercado tiene un excedente de producción de energía, la empresa de servicios públicos (o el participante donde está prestando su infraestructura de red) recibe un porcentaje de la transacción equivalente al 1% del excedente total. La nueva tarifa refleja el precio real de la producción de energía considerando la región geográfica sin subsidios. La Tabla **4-20** muestra una comparación usando las tarifas reales con las nuevas tarifas usando nuestra propuesta de TES en SMI usando blockchain para los consumidores domésticos. Los costos reflejados son el promedio de las transacciones totales en cada tarifa y están expresados en Pesos Mexicanos (MXN). Observe que las tarifas iniciales 1, 1A, 1B, donde el costo con la nueva tarifa es ligeramente superior al original, pero las últimas tarifas 1C, 1D, 1E, 1F y DAC son mejores y disminuyen con la alta demanda. En realidad, en las tarifas domésticas mexicanas solo el 1.27% del consumidor tiene un sistema DER en casa, pero con una mayor penetración renovable el porcentaje de reducción podría incrementarse significativamente.El procentaje promedio de reducción es del 15.02% que se puede apreciar en las tarifas más caras, mientras que en las tarifas bajas hay un pequeño incremento de 1.88%.

Tabla 4-20 *Comparativa usando TES en tarifas mexicanas.*

Tarifa	Costos promedios con las tarifas actuales	Costos con las tarifas propuestas	Porcentaje de reducción
1	$377.14	$389.67	+3.32
1A	$401.67	$405.92	+1.06
1B	$527.35	$530.71	+0.64
1C	$633.19	$632.16	-0.16
1D	$748.26	$744.25	-0.54
1E	$893.49	$867.43	-2.92
1F	$1,127.61	$1,053.66	-6.56
DAC	$1,532.27	$1,381.12	-9.87

Capítulo 5 Conclusiones y trabajos futuros

En este capítulo se muestran las principales conclusiones del trabajo, así como los productos obtenidos del mismo. Además, se delinean posibles trabajos a desarrollar en el futuro.

5.1 Conclusiones

La medición de energía eléctrica y en general de cualquier sistema de medición es vital para la facturación y cobro de los servicios que se brindan. La correcta medición del sumistro eléctrico es fundamental para la confianza entre las empresas eléctricas y los usuarios finales. En este sentido, la ciberseguridad de las transacciones y datos del SMI es sumamente importante para el éxito de los SMI, aunque también se deben considerar otros factores:

1. El acceso a la aplicación del SMI debe ser accesible a través de varios dispositivos y adaptarse a las diferentes capacidades de visualización y procesamiento.
2. La información sobre el consumo y la producción de electricidad debe mostrarse de forma sencilla. El análisis de datos debe realizarse y mostrarse gráficamente. Es imperativo que el usuario pueda interactuar con sus diferentes electrodomésticos de alto consumo como refrigeradores, aires acondicionados, calentadores, planchas, lavadoras, sistemas de iluminación, entre otros. Esta interacción debe mostrar muy claramente cuánta energía (y especialmente dinero) se está utilizando cuando uno u otros dispositivos están encendidos.
3. Se deben considerar aspectos de la interacción social, como mostrar a los clientes en las redes sociales la facturación de un período a otro, ver cómo ese consumo mejoró y la socialización de diversos aspectos del servicio eléctrico.
4. Para los clientes residenciales mexicanos, es fundamental que las interfaces SMI permitan conocer los costos de la electricidad en todo momento. En México, aunque ya existen algunos lugares que cuentan con SMI, su uso en el país no está muy extendido, por lo que será necesario contar con una campaña de presentación que muestre todas las posibles ventajas de estos sistemas ya que el usuario mexicano en general es extremadamente reacio a instalar nuevos medidores inteligentes.
5. Los SMI deben integrarse fácilmente con diversas tecnologías del hogar inteligente para poder interactuar con estos dispositivos y, sobre todo, conocer su consumo eléctrico y los costes que conlleva dicho consumo.
6. El desarrollo de SMI debería incluir tecnologías disruptivas que, en los últimos años, han revolucionado nuestra vida diaria. Entre estas tecnologías se encuentran las cadenas de bloques que permiten que la información se almacene de forma segura. Derivado del concepto de cadenas de bloques, surge el concepto de sistemas de energía transaccional, que permite a los prosumidores comercializar entre sí la energía producida a partir de fuentes renovables utilizando esquemas de criptomonedas. Por ello, es necesario que los SMI cuenten con una amplia variedad de métodos de pago y que se actualicen con frecuencia.
7. El SMI debe estar integrado con los VE para medir su alto consumo de energía eléctrica y, sobre todo, permitir la e-movilidad de cualquier carga eléctrica,

especialmente aquellas de alto consumo y que sean fáciles de mover. Por ejemplo, mañana, si un amigo quiere conectar su VE en nuestra casa, este elevado consumo de energía eléctrica y, por tanto, elevado coste, podrá ser facturado y cargado a su cuenta de su empresa eléctrica.

8. El desarrollo de hardware de medidores inteligentes debe considerar que, a diferencia de los medidores tradicionales que podrían durar toda la vida, los medidores inteligentes tienen una vida útil de 10 años debido a la rápida obsolescencia del hardware. Por esta razón, los medidores deben actualizar continuamente su software. Por otro lado, para que los medidores inteligentes tengan una mayor penetración en el mercado, necesitan tener una mayor funcionalidad. Para ello, se pueden integrar sensores como temperatura, humedad, movimiento, o incluso una cámara de video para ayudar a nuevas aplicaciones como el control climático y la videovigilancia.
9. Los SMI deben ser lo suficientemente inteligentes para poder adaptarse a diferentes tipos de clientes con diferentes tipos de roles y características. Por ello, deben contar con la capacidad informática suficiente para llevar a cabo procesos de inteligencia artificial y el despliegue de interfaces de usuario amigables que mejoren la experiencia de los usuarios en el uso de la energía eléctrica en hogares, oficinas e industria.

La introducción de cadenas de bloques a SMI en particular en AMI como un mecanismo de seguridad cibernética y confiable puede traer múltiples beneficios, siendo una de estas mitigaciones de manipulación de BD. Para poder implementar la cadena de bloques en SMI, la cadena de bloques debe adaptarse a todas las capas de SMI, particularmente en lo que respecta a SMI y otros dispositivos de IoT que se administran en REI.

En este trabajo, se ha propuesto una arquitectura novedosa para SMI de diseño seguro utilizando cadenas de bloque. Esta arquitectura propone el uso de una cadena de bloques multinivel en SMI (HAN, NAN, FAN/WAN, centro de datos) utilizando un algoritmo de consenso ligero privado: Prueba de Eficiencia, que está optimizado para dispositivos IoT y de baja energía (limitados en recursos) pero también adaptable a otros dispositivos en SMI. Esta arquitectura propone el uso de BD en el MI que actualmente no es común. La protección de datos se logra mediante el uso de una cadena de bloques de varios niveles y una estructura de datos simple que incluye el cifrado de las transacciones de energía. La arquitectura propuesta podría usarse para la próxima generación de sistemas AMI porque incluye una ciberseguridad más sólida para la manipulación de datos en las transacciones de energía.

Por otra parte, la próxima generación de aplicaciones para REI y SMI necesita un procesamiento analítico mejorado. Una solución posible y factible consiste en segmentar AMI en niveles para aumentar las capacidades de procesamiento, almacenamiento y comunicación. Además, la velocidad y la granularidad de los datos también son importantes para procesar el análisis de datos de forma eficaz. La arquitectura propuesta en este documento mostró que la arquitectura borde-niebla-nube es una solución viable para aplicaciones de SMI que ofrece ventajas de procesamiento de datos mediante el uso de múltiples niveles. La metodología resultante puede realizar análisis de datos para una variedad de aplicaciones en SMI. Se probó la arquitectura del sistema para tres aplicaciones diferentes (pronóstico de consumo/producción de energía, calidad de energía y robo de energía). La primera aplicación se mejoró de 51.09% a 63.29% de puntuación final, la segunda aplicación se mejoró de 90.53% a 98.17% y la última aplicación se mejoró de 88.16% a 90.61%. Los resultados sugieren que otros procesos relacionados con la producción, transmisión, distribución y consumo de energía pueden beneficiarse de la implementación de la arquitectura propuesta. Además, este trabajo demostró que era posible implementar una arquitectura de SMI de varios niveles para el análisis de datos utilizando datos en tiempo real y en tiempo diferido. La arquitectura propuesta es versátil y se puede utilizar para implementar diferentes procedimientos de formación y aprendizaje para el desarrollo de modelos en línea y fuera de línea capaces de adaptarse a diferentes entornos mediante el uso del aprendizaje por refuerzo.

A su vez, el diseño de tarifas de energía eléctrica es un esquema bastante complejo que debe tomar todas las fuentes de costos y, a su vez, debe garantizar la sostenibilidad de la disponibilidad de energía eléctrica a precios justos. Para que el SEP continúe con los criterios de eficiencia, calidad, confiabilidad, continuidad, seguridad y sustentabilidad, es necesario implementar nuevos procedimientos y tecnologías que sean rentables y le ayuden a lograr estos objetivos. El comportamiento de los usuarios está cambiando cada vez más y casi la mayoría de las tecnologías actuales y el SEP no es la excepción. Por esta razón, los resultados sugieren que la implementación de las TES propuestas puede ofrecer ventajas competitivas tanto para los nuevos prosumidores como para los usuarios finales, permitiendo compartir el excedente de electricidad y reducir la facturación. Además, los resultados sugieren que la combinación de la infraestructura de cadenas de bloques y SMI puede resultar en mejoras sustanciales de la funcionalidad de los TE. La implementación de estas soluciones puede contribuir a mejores sistemas de calificación y ahorros de aproximadamente el 15% del costo total de los consumos en México. El uso de TES con la solución de cadena de bloques y otras tecnologías aumentará en todo el mundo en beneficio de todos los participantes del mercado de la electricidad.

5.2 Trabajos futuros

Con base en lo desarrollado se propone mejorar la ciberseguridad de las transacciones de medición a través de uso de esquemas de criptografía más robustos, principalmente pensando en más privacidad de las transacciones (anonimato) y utilizando esquemas que sean resistentes ante la inminente llegada de computadoras cuánticas.

Se sugiere seguir trabajando en esquemas de blockchain, particularmente en el área de la nube con la idea de ser más escalables e interoperables usando plataformas abiertas y/o comerciales que permitan mayor interoperabilidad entre sistemas de cadenas de bloques.

Es necesario mejorar los componentes de la cadena de bloques a fin de que la infraescturctura de los SMI pueda ser integrado con otras aplicaciones que involucren ML y DA dentro del área de la REI, como lo son la detección y localización de fallas, monitoreo, respuesta a la demanda, pronóstico en tiempo real de consumo entre otras aplicaciones.

5.3 Productividad lograda

A continuación, se presenta la numeralia alcanzada con este trabajo doctoral. En primera instancia se muestran las publicaciones relevantes y por otra parte la formación de recursos humanos en investigación.

La Tabla **5-1**, muestra los resultados principales de las publicaciones tecno-científicas derivadas de este trabajo doctoral.

5.3.1 Publicaciones en Revistas JCR

1. Juan C. Olivares-Rojas, Enrique Reyes-Archundia, José A. Gutiérrez-Gnecchi, Jaime Cerda-Jacobo, and Johan W. González-Murueta, “A Novel Multi-Tier Blockchain Architecture to Protect Data in Smart Metering Systems”, IEEE Transactions on Engineering Management, Special Issue on Blockchain Ecosystems, vol. 67, no. 4, Nov. 2020, doi: 10.1109/TEM.2019.2950410.

2. Juan C. Olivares-Rojas, Enrique Reyes-Archundia, Jose A. Gutiérrez-Gnecchi, Johan W. González-Murueta, Jaime Cerda-Jacobo, “A multi-tier architecture for data analytics in smart metering systems”, Simulation Modelling Practice and Theory, special issue on IoT, Cloud, Big Data and AI in Interdisciplinary Domains , Elsevier, Vol. 102, July 2020, doi: 10.1016/j.simpat.2019.102024.

Tabla 5-1 *Resultados principales de publicaciones derivadas de este trabajo.*

Concepto	**Cantidad**
Publicaciones en Revistas JCR (autor principal)	6
Publicaciones en revistas arbitradas e indexadas en otros índices (autor principal)	9
Publicaciones en revistas arbitradas por aparecer (autor principal)	1
Publicaciones en revistas arbitradas e indexadas en otros índices (coautor)	2
Capítulos de libro (autor principal)	2
Memorias en extenso de congreso internacional (autor principal)	7
Publicaciones por aparecer en memorias en extenso de congreso internacional (autor principal).	1
Memorias de Congreso en Extenso (coautor)	7
Publicación en Revista de Divulgación (autor principal)	1
Publicaciones en Poster (autor principal)	1
Colaborador de Proyectos de Investigación con Financiamiento (TecNM)	5

3. Juan C. Olivares-Rojas, Enrique Reyes-Archundia, José A. Gutiérrez-Gnecchi, Jorge L. Diaz-Huerta, Jaime Cerda-Jacobo, Adriana C. Téllez-Anguiano, Johan W. González-Murueta, “Data Analytics of Electromagnetics Field Measurements in Smart Meters”, International Journal of Combinatorial Optimization Problems and Informatics, Vol. 11, No. 2, 2020, Indexado en Clarivate Emerging Source Citation Index (ESCI) y CONACyT, https://ijcopi.org/ojs/article/view/165.

4. Juan C. Olivares-Rojas, Enrique Reyes Archundia, José A. Gutiérrez-Gnechi, Ismael Molina-Moreno, Jaime Cerda-Jacobo, Arturo Méndez-Patiño, "Towards Cybersecurity of the Smart Grid using Digital Twins", IEEE Internet Computing, doi: 10.1109/MIC.2021.3063674

5. Juan C. Olivares-Rojas, Enrique Reyes Archundia, José A. Gutiérrez-Gnechi, Ismael Molina-Moreno, Jaime Cerda-Jacobo, Arturo Méndez-Patiño, "A Transactive Energy Model for Smart Metering Systems using Blockchain", CSEE Journal of Power & Energy Systems, Vol. 7, No. 5, doi: 10.17775/CSEEJPES.2020.05670

6. Juan C. Olivares-Rojas, Enrique Reyes Archundia, José A. Gutiérrez-Gnechi, Ismael Molina-Moreno, Jaime Cerda-Jacobo, Arturo Méndez-Patiño, "A Methodology for Cyber Hygiene in Smart Grids", Revista Dyna Ingeniería e Industria, https://www.revistadyna.com/Reports/ArticulosDirectricesEvaluacion.aspx.

5.3.2 Publicaciones en revistas arbitradas e indexadas en otros índices (autor principal)

1. Juan C. Olivares-Rojas, Enrique Reyes-Archundia, José A. Gutiérrez-Gnecchi, Johan W. González-Murueta, Jaime Cerda-Jacobo, Adriana C. Téllez-Anguiano, "A Comparative Assesment of Cryptography Algorithms for Data Analytics Applications in Smart Metering", Segundas Jornadas de Ciencia y Tecnología, Cenidet, Cuernavaca, Morelos, ISSN en trámite, 5 de abril de 2019, https://jcyta.cenidet.tecnm.mx/revistas/jcyta/02-Revista_JCyTA_Vol-2-Num-1_Ene-Jun_2019.pdf.

2. Juan C. Olivares-Rojas, Enrique Reyes-Archundia, José A. Gutiérrez-Gnecchi, Johan W. González-Murueta, Adriana C. Téllez-Anguiano, Jaime Cerda-Jacobo, "Analítica de datos en simulador de redes para sistemas de medición inteligente", Memoria del Congreso COMIA 2019, Research in Computer Science, ISSN: 1870-4069, Vol. X. No. X, pp. 9, Tepic, Nayarit, México, 2019, doi: 10.13053/rcs-148-8-18.

3. Juan C. Olivares-Rojas, Enrique Reyes-Archundia, José A. Gutiérrez-Gnecchi, Francisco Reyes-Calderón, "Propuesta de Flexibilidad Curricular en el Tecnológico Nacional de

México", Memorias del Congreso ANFEI 2019, Revista ANFEI Digital, ISSN 2395-9878, Vol. 2019, No. 11, Veracruz, Veracruz, México,2019, https://www.anfei.mx/revista/index.php/revista/article/view/529.

4. Juan C. Olivares-Rojas, José A. Noriega-Carmona, Enrique Reyes-Archundia, José A. Gutiérrez-Gnecchi, "Usabilidad y experiencia de usuario en un portal de un sistema de medición inteligente", Revista de la Alta Tecnología y Sociedad, Vol 11, No, 1, pp. 9-17, 2019, ISSN: 1940-2171, http://www.academiajournals.com/revista-alta-tec-y-sociedad

5. Juan C. Olivares-Rojas, Enrique Reyes-Archundia, Sergio A. Carrillo-Villanueva, José A. Gutiérrez-Gnecchi, "Propuesta de Mercado Eléctrico Minorista Transactivo en México", Revista Identidad Energética 2019, vol. 1, no. 2, ISSN: 2448-7775, http://cinergiaug.org/Revista/VI_2019/RIE_VII_N1_Dic2019_2.pdf.

6. Juan C. Olivares-Rojas, Enrique Reyes-Archundia, José A. Gutiérrez-Gnecchi, Ismael Molina-Moreno, Jaime Cerda-Jacobo, "UNA REVISIÓN A LA CIBER SEGURIDAD EN REDES ELÉCTRICAS INTELIGENTES", Revista Pistas Educativas, Vol. 41, No. 135, Instituto Tecnológico de Celaya, ISSN: 448-847X, http://www.itcelaya.edu.mx/ojs/index.php/pistas/article/view/2261/0.

7. Juan Carlos Olivares Rojas, Enrique Reyes Archundia, José Antonio Gutiérrez Gnecchi, Ismael Molina Moreno and J. Guadalupe Ramos Díaz, "A SURVEY ON SMART METERING SYSTEMS USING HUMAN-COMPUTER INTERACTION", Revista Memoria Electro, Electro vol. 42, ISSN: 1405-2172, Instituto Tecnológico de Chihuahua, octubre de 2020, http://electro.itchihuahua.edu.mx/memorias_electro/revista.htm

8. Juan C. Olivares-Rojas, Enrique Reyes-Archundia, José A. Gutiérrez-Gnecchi, Ismael Molina-Moreno, Adriana C. Téllez-Anguiano, Jaime Cerda-Jacobo, "Smart Metering System Data Analytics using Multicore Edge Computing", International Journal of Reconfigurable and Embedded Systems (IJRES), DOI: 10.11591/ijres.v10.i1.pp11-17, ISSN: 2089-4864.

9. Juan C. Olivares-Rojas, Enrique Reyes-Archundia, José A. Gutiérrez-Gnecchi, Ismael Molina-Moreno, J. Guadalupe Ramos-Díaz, J. Gabriel González-Serna, "Towards human-computer interaction on smart metering systems", Revista Avances en Interacción Humano-Computadora, vol. 5, no. 1, noviembre 2020, DOI: 10.47756/aihc.y5i1.58.

5.3.3 Publicaciones en revistas arbitradas e indexadas en otros índices (coautor).

1. Anastacio Antolino-Hernández, Cristhian Torres-Millarez, Heberto Ferreira-Medina, Juan C. Olivares-Rojas, "Gestión de documentos digitales con firma encriptada, mediante el uso de PKI centralizado, y distribuido utilizando blockchain para un intercambio seguro", Revista de Cómputo-Informatica y Software de la Editorial Ecorfan, vol. 5, no. 15, 2019, DOI: 10.35429/JRD.2019.15.5.26.37.

2. Monserrat Yazmín Loya Ayala, Juan Carlos Olivares Rojas, Enrique Reyes Archundia, Ana Lilia Mendieta Jiménez and María Cristina Jasso Carbajal, "Analítica de datos para pronóstico de robo de energía usando medidores inteligentes", Congreso de Investigación Multidisciplinaria 2019, por aparecer en la Revista CIM 2019, Vol. 7, No. 1, pp. 1918-1925, ISSN: 2007-8102, https://drive.google.com/file/d/1FZgsZI5YuXFIP1g6F21n0CjnVrKa4wxz/view

5.3.4 Publicaciones en revistas arbitradas e indexadas aceptadas en espera de publicación (autor principal)

1. Juan C. Olivares-Rojas, Enrique Reyes-Archundia, José A. Gutiérrez-Gnecchi, "Cyber Security on Transactions in Smart Metering Systems Using Blockchain", Consorcio Doctoral de MICAI (Mexican International Conference on Artificial Intelligence), Revista Research in Computer Science, IPN, Vol., No. x.

5.3.5 Capítulos de libro (autor principal).

1. Juan C. Olivares-Rojas, Luis E. Ruíz-Martínez, Enrique Reyes-Archundia, José A. Gutiérrez-Gnecchi, Ismael Molina-Moreno, "Arquitectura de un lago de datos para Sistemas de Medición Inteligente", libro "Aplicaciones de la Computación", Universidad Autónoma de Coahuila, agosto de 2020. ISBN: 978-607-506-395-9, https://drive.google.com/file/d/1C7nDyqKkZzHinSZd2fifABi-lA64vSY-/view.

2. Juan C. Olivares-Rojas, Enrique Reyes-Archundia, José A. Gutiérrez-Gnecchi, Ismael Molina-Moreno, Arturo Méndez-Patiño, Jaime Cerda-Jacobo. "Forecasting electricity consumption using weather data in an edge-fog-cloud data analytics architecture", Advances on P2P, Parallel, Grid, Cloud and Internet Computing. 3PGCIC 2020. Lecture Notes in Networks and Systems, vol. 158, DOI: 10.1007/978-3-030-61105-7_41, Yonago, Japón, Octubre 2020.

5.3.6 Publicación en memorias en extenso de congreso internacional (autor principal).

1. Juan Carlos Olivares-Rojas, Enrique Reyes-Archundia, Ismael Molina-Moreno, José Antonio Gutiérrez-Gnecchi, Adriana Téllez-Anguiano, Jaime Cerda-Jacobo and Mario Heras-Cervantes, "A Comparative Assessesment of Blockchains in Embedded Systems", 2018 IEEE International Autumn Meeting on Power, Electronics and Computing (ROPEC), Ixtapa-Zihuatanejo, México, Noviembre 14-16 de 2018, DOI: 10.1109/ROPEC.2018.8661372.

2. Juan C. Olivares-Rojas, José A. Noriega-Carmona, Enrique Reyes-Archundia, José A. Gutiérrez-Gnecchi, "Aplicación de Técnicas de UX en el Diseño de un Portal de un Sistema de Medición Inteligente", Memorias del Congreso Internacional de Investigación Academia Journals Tepic 2019, ISSN: 1946-5351, Vol. 11, No. 1, pp. 1026-1031, 2019, Tepic, Nayarit, México, https://drive.google.com/drive/folders/1D11R0KEIUiyeDUCrbvseb3Vr1DoN1OEY.

3. Juan C. Olivares-Rojas, Enrique Reyes-Archundia, José A. Gutiérrez-Gnecchi, Ismael Molina-Moreno, "A Survey on Smart Metering Blockchain for E-Mobility" Electircal Vehicles International Symposium, septiembre 2020, https://arxiv.org/abs/2009.09075.

4. Juan C. Olivares-Rojas, Enrique Reyes-Archundia, Nol E. Rodríguez-Maya, José A. Gutiérrez-Gnecchi, Ismael Molina-Moreno, Jaime Cerda-Jacobo, "Machine Learning Model for the Detection of Electric Energy Fraud using an Edge-Fog Computing Architecture", IEEE Conference Engineering Vereacruz (ICEV) 2020, octubre de 2020, DOI: 10.1109/ICEV50249.2020.9289669.

5. Juan C. Olivares-Rojas, Enrique Reyes-Archundia, Jesús E. Alcaraz-Chávez, Andrés Villagómez-Rios, José A. Gutiérrez-Gnecchi, "Detección de Movimiento usando Medidores Inteligentes en el 15vo. Congreso Nacional de Ciencia, Tecnología e Innovación, del ICTI Michoacán, del 28 al 30 de octubre de 2020, https://drive.google.com/file/d/1ujLaUkWtvM5ej1W-s3a1byMCwAqD7LVN/view.

6. Juan C. Olivares-Rojas, Enrique Reyes-Archundia, José A. Gutiérrez-Gnecchi, Ismael Molina-Moreno, J. Gabriel González-Serna. "Improvement of forecasting and classification in smart metering systems using a neural compute stick", 2020 IEEE Autumn Meeting on Power, Electronics and Computing (ROPEC 2020), DOI: 10.1109/ROPEC50909.2020.9258745.

7. Juan C. Olivares-Rojas, Enrique Reyes Archundia, José A. Gutiérrez-Gnechi, Ismael Molina-Moreno, Jaime Cerda-Jacobo, Arturo Méndez-Patiño, "A Comparative Assessment of Embedded Databases for Smart Metering Systems", IEEE Innovative Smart Grid Technologies Latin America (ISGT-LA) 2021, doi: 10.1109/ISGTLatinAmerica52371.2021.9543058

5.3.7 Publicaciones por aparecer en memorias en extenso de congreso internacional (autor principal).

1. Juan C. Olivares-Rojas, Enrique Reyes-Archundia, José A. Gutiérrez-Gnecchi, Ismael Molina-Moreno, Jaime Cerda-Jacobo, Arturo Méndez-Patiño, "A VAR model to forecast electricity consumption in Smart Metering System using an edge-fog-cloud architecture", Mexican International Conference on Artificial Intelligence (MICAI) 2021, http://www.micai.org/2021/.

5.3.8 Artículos en memoria de congreso en extenso (coautor).

1. Xavier Arroyo Rodríguez, Juan Carlos Olivares Rojas, Enrique Reyes Archundia, José Antonio Gutiérrez Gnecchi, Arturo Méndez Patiño, "Estudio Comparativo de Protocolos de Comunicación en Banda Estrecha en Líneas de Potencia", Congreso Academia Journals Celaya 2017, vol. 9, no. 6, ISSN: 1946-5351, pp. 394-402 https://drive.google.com/file/d/1UB1Y8XQAIQTooSV1T4Tj9RKLJPq3RqRc/view.

2. Cristhian Nivardy Marín Chávez, Juan Carlos Olivares Rojas, Enrique Reyes Arhundia, José Antonio Gutiérrez-Gnecchi, Gabriela Lua Vargas, Nestor Francisco Guerrero Rodríguez, "Estudio Comparativo de Dispositivos Digitales y Aplicaciones para la Gestión de Base de Datos", Congreso Academia Journals Celaya 2017, vol. 9, no. 6, ISSN: 1946-5351, pp. 3822-3827, https://drive.google.com/file/d/1wMAG7bzRsMtvWEx5__Dqi8Ao4Au3gYbH/view.

3. Juan C. Zavala-Ramos, Juan C. Olivares-Rojas, Enrique Reyes-Archundia, Cristhian Torres-Millarez, Anastacio Antolino-Hernández, "Robustecimiento de la Placa Raspberry Pi para Aplicaciones en el Internet de las Cosas", 13avo. Congreso Estatal de Ciencia, Tecnología e Innovación 2018, Morelia, Michoacán, México, octubre 18-19, 2018, https://mega.nz/#!4YJxHYST!fRft_w5iXkV5jtT7Vbkksvt501SW-cKQTEiWVJsEv8Y.

4. Cristhian N. Marín-Chávez, Juan C. Olivares-Rojas, Enrique Reyes-Archundia, Ismael MolinaMoreno, José A. Gutiérrez-Gnecchi, "Comparativa de Base de Datos para Sistema de Monitoreo en Medidores Inteligentes", 13avo. Congreso Estatal de Ciencia, Tecnología e Innovación 2018, Morelia, Michoacán, México, octubre 18-19, 2018, https://mega.nz/#!4YJxHYST!fRft_w5iXkV5jtT7Vbkksvt501SW-cKQTEiWVJsEv8Y.

5. Jorge L. Reyes-González, Enrique Reyes-Archundia, Juan C. Olivares-Rojas, José A. Gutiérrez-Gnecchi, Johan W. González-Murueta, "Diseño de una arquitectura de preprocesamiento de datos en medidores inteligentes para pruebas y entrenamientos de algoritmos de inteligencia de datos", Memorias del Congreso Internacional de Investigación Academia Journals Morelia 2019, ISSN: 1946-5351, Vol. 11, No. 2, pp. 2379-2384, 2019, Morelia, Michoacán, México, https://static1.squarespace.com/static/55564587e4b0d1d3fb1eda6b/t/5e306ae487c8e752f5fb3d74/1580231443304/Memorias+del+Congreso+Morelia+2019+-+Academia+Journals+-+Tomo+15.pdf

6. Ana Liliana Rodríguez Ancelmo, Juan Carlos Olivares Rojas, Noel Enrique Rodríguez Maya, Enrique Reyes Archundia, Jesús Eduardo Alcaraz Chávez, José Antonio Gutiérrez-Gnecchi, "Modelos de Predicción de Lecturas de Consumo/Producción de Energía Eléctrica

para Detectar Fraudes de Energía", Congreso ICTI 2019, ISSN: en trámite, https://mega.nz/#!5BZ2hSSI!QjshCuS3Sh8SAFAwjDG5_-rdCH9a8Fydb6pHvxZMDdY.

7. Marisol Alemán Duarte, Enrique Reyes Archundia, Juan Carlos Olivares Rojas, José Antonio Gutiérrez Gnecchi, Rafael Lara Hernández, "Análisis de datos locales como alternativa para disminuir la sobreproducción eléctrica en México", en el Congreso Academia Journals Morelia 2020, Vol. 12, no. 1, ISSN: 1946-5351, pp. 47-51, https://static1.squarespace.com/static/55564587e4b0d1d3fb1eda6b/t/5ec5c0562706f13e3f5ef978/1590018203759/Tomo+01+-+Memorias+Academia+Journals+-+Morelia+2020.pdf

5.3.9 Publicación en revista de divulgación (autor principal).

1. Juan C. Olivares-Rojas, Enrique Reyes-Archundia, José A. Gutierrez-Gnecchi, Ismael Molina-Moreno, Adriana Téllez-Anguiano, "Is the Blockchain a good solution for Cybersecurity in the Smart Grid?", IEEE Smart Grid Newsletter, Julio de 2018, http://resourcecenter.smartgrid.ieee.org/sg/product/publications/SGNL0256.

5.3.10 Publicaciones en Póster (autor principal)

1. Juan C. Olivares Rojas, Enrique Reyes-Archundia, José A. Gutiérrez-Gnecchi, Johan W. González-Murueta, and Adriana Téllez-Anguiano, "Data Analytics in Smart Meters for the Detection of Energy Theft", Reunión Internacional de Inteligencia Artificial y sus Aplicaciones RIIAA, 30 de agosto de 2019, https://openreview.net/forum?id=rkeWehEegr

5.3.11 Colaborador de Proyectos de Investigación con Financiamiento (TecNM)

1. Enrique Reyes Archundia, Juan Carlos Olivares Rojas, Javier Correa Gómez, 5793.16-P: "Investigación de Métodos de Comunicación para el Diseño de Medidores Inteligentes", 02/05/2016 – 02/05/2018.

2. Ismael Molina Moreno, Juan Carlos Olivares Rojas, Enrique Reyes Archundia, 6526.18-P: "Cyber Seguridad en Medidores Inteligentes (Smart Meters) utilizando Cadenas de Bloques", 01/01/2018 – 31/12/2018.

3. Johan W. González-Murueta, Juan C. Olivares-Rojas, Enrique Reyes-Archundia. 6385.19-P: "Analítica de datos en medidores inteligentes para determinar patrones de consumo/producción para mejorar la eficiencia energética y evitar robo de energía", 01/01/2019 – 31/12/2019.

4. Ismael Molina Moreno, Juan Carlos Olivares Rojas, Enrique Reyes Archundia, 8000.20-P: "Modelos de Aprendizaje Máquina para la Detección de Consumos/Producción Anómalos de Energía Eléctrica utilizando una Arquitectura de Cómputo en la Niebla", 01/01/2020 – 31/12/2020.

5. Ismael Molina Moreno, Juan Carlos Olivares Rojas, José Antonio Gutiérrez Gnecchi, 10285.21-P: "Sistema de Medición Inteligente, Transactivo y Desagregado de Consumo/Producción de Energía Eléctrica", 01/01/2021 – 31/12/2020.

En lo que refiere a la formación de recursos humanos se cuentan con los siguientes resultados, mostrados en la Tabla **5-2**.

5.3.12 Tesis de maestría co-dirigida

1. Xavier Arroyo Rodríguez, "Estudio de Vulnerabilidades a Nivel Físico y de Enlace en Protocolos G3_PLC y PRIME-PLC para Comunicación por Línea de Potencia", 18 de Febrero de 2019, Maestría en Ciencias en Ingeniería Electrónica, Instituto Tecnológico de Morelia, http://sagitario.itmorelia.edu.mx/pelectron/documentos/X-Arroyo.pdf

2. Cristhian Nivardy Marín Chávez, "Estudio Comparativo de Base de Datos Empotradas para Aplicaciones de Medidores Inteligentes", febrero 2020, Maestría en Ciencias en Ingeniería Electrónica, Instituto Tecnológico de Morelia.

Tabla 5-2 *Resultados principales de formación de recursos humanos*

Concepto	**Cantidad**
Tesis de maestría co-dirigida:	2
Sinodal titulación licenciatura	2
Asesor de Residencias Profesionales	7
Participación de asesor en veranos de investigación	3 (6)
Asesoría de alumnos de Servicio Social	4 (5)
Conferencias dictadas	7
Participación en Proyectos de Innovación	1

5.3.13 Sinodal en titulación en Licenciatura.

1. "Estudio de Protocolos de Comunicación para Redes Inteligentes" Francisco Javier Anguiano de Licenciatura en Informática, Instituto Tecnológico de Morelia.

2. "Propuesta de Mercado Eléctrico Minorista usando Blockchain y Analítica de Datos", Sergio Adrián Carrillo Villanueva, Ing. Eléctrica, Instituto Tecnológico de Morelia, fungiendo como coasesor del trabajo con tutela del Dr. José Luis Monroy Morales (asesor interno) del Depto. de Ing. Eléctrica.

5.3.14 Asesor en residencias profesionales.

1. César Andrés Covarrubias Cisneros, "Cyber Seguridad en Medidores Inteligentes (Smart Meters) utilizando Cadenas de Bloques", Ing. en Tecologías de la Información y Comunicaciones, Instituto Tecnológico de Estudios Superiores de Zamora.

2. Salvador Hernández López, “Desarrollo de Interfaces Web Adaptativas para Medidores Inteligentes”, Ing. en Sistemas Computacionales, Instituto Tecnológico de Estudios Superiores de Zamora.

3. Julio César Ortega Contreras, “Implementación de Cadenas de Bloques usando Hyperledger para Transacciones de Consumo Eléctrico”, Ing. en Sistemas Computacionales, Instituto Tecnológico Morelia.

4. Sergio Adrián Carrillo Villanueva, “Propuesta de Mercado Eléctrico Minorista usando Blockchain y Analítica de Datos”, Ing. Eléctrica, Instituto Tecnológico de Morelia.

5. Ana Liliana Álvarez Anselmo, “Modelo de predicción de lecturas de consumo/producción de energía eléctrica anómalos”, Ing. en Sistemas Computacionales, Instituto Tecnológico de Zitácuaro.

6. Eréndira del Carmen Jiménez Toscano, Instituto Tecnológico Superior de los Ríos, “Analítica de datos en medidores inteligentes para determinar patrones de consumo/producción para mejorar la eficiencia energética y evitar robo de energía”.

7. Nancy Cortés García, “Diseño de un Medidores Inteligente de Energía Eléctrica”, Ing. en Electrónica, Instituto Tecnológico de Morelia.

5.3.15 Participación como asesor en veranos de investigación.

1. Juan Carlos Zavala Ramos, Instituto Tecnológico Superior de Puruándiro, “Robustecimiento de la Placa Raspberry Pi 3”, Programa Delfín 2018.

2. Miriam Zamora Álvarez, Jesús Samael Mora Lemus y Romeo Jafet Ascencio Alonso, Instituto Tecnológico Superior Purépecha, “Sistema de Monitoreo para Medidores Inteligentes (Smart Meters)”, Programa Delfín 2018.

3. Monserrat Yazmín Loya Ayala de la Universidad Politécnica del Valle de Toluca de la carrera de Ing. Industrial y Eréndira del Carmen Jiménez Toscano del Instituto Tecnológico Superior de Los Rios, en Tabasco, de la carrera de Ing. en Sistemas Computacionales con el proyecto: "Analítica de Datos para Pronóstico de Robo de Energía usando Medidores Inteligentes", Programa Delfín 2019.

5.3.16 Asesoría de alumnos de Servicio Social.

1. Andrés Villagómez Ríos, "Implementación de Seguridad Física en Medidores Inteligentes", Instituto Tecnológico de Morelia

2. Katia Lidia Martínez Olvera, "Aplicación para recolección de datos de medidores en un concentrador de datos", Instituto Tecnológico de Morelia

3. José Luis Chávez Ceballos, Wilfrido Cortés Orozco, "Implementación de Blockchain en Concentradores de Datos", Instituto Tecnológico de Morelia.

4. Isaí Gutiérrez Rubio, Instituto Tecnológico de Morelia.

5. Cristhian Vargas Buenrostro, "Investigación de Algoritmos de Cifrado en Raspberry 4", Ing. en Sistemas Computacionales, Instituto Tecnológico de Morelia.

5.3.17 Conferencias dictadas.

1. "Evaluación de Criptomonedas y Mecanismos de Cadenas de Bloques para su Uso en Sistemas de Transacciones Segura en Mercados Eléctricos Minoristas", impartido en noviembre en el Instituto Tecnológico Superior de Ciudad de Hidalgo, 2017.

2. "Ciber Seguridad en Redes Eléctricas Inteligentes" impartido en el Congreso Tehkne 2017 en el Instituto Tecnológico de Morelia, octubre de 2017.

3. “Ciber Seguridad Utilizando Cadenas de Bloques” en marzo de 2018 en el Instituto Tecnológico Superior de Pátzcuaro.

4. “Internet de las Cosas en Redes Eléctricas inteligentes (Smart Meters)”, Instituto Tecnológico de Jiquilpan, 3 de octubre de 2018 (ver evidencia 21).

5. “Analítica de Datos en Dispositivos de Internet de las Cosas (IoT)”, Instituto Tecnológico Superior de Ciudad Hidalgo, marzo de 2019.

6. “Análisis de Datos usando Single Board Computers”, Data day 2019, 21 de marzo de 2019.

7. “Analítica de Datos en IoT”, Instituto Tecnológico Superior de Puruándiro, 23 de mayo de 2019.

5.3.18 Participación en proyectos de innovación.

1. Convocatorias de Siemens: “Convocatoria para el desarrollo de ideas con investigadores” y “Blockchain and Energy Transformation Challenge”. En donde se quedaron en los primeros 10 lugares y donde además de recibir capacitación referente a innovación tecnológica se obtuvo de la primera convocatoria un estudio de inteligencia competitiva como premio.

Referencias

[1] IEEE (2019), "IEEE is Fueling the Fourth Industrial Revolution", Disponible en línea: https://innovate.ieee.org/innovation-spotlight-ieee-fueling-fourth-industrial-revolution/?LT=XPLHL_XPL_1.2019_LM_Innovation_Spotlight_4IR, consultado: agosto 2021

[2] G. Vial (2019), "Understanding digital transformation: A review and a research agenda". *The Journal of Strategic Information Systems*, vol. 28, no. 2, pp. 118-144, doi: 10.1016/j.jsis.2019.01.003.

[3] G. Dileep (2020), "A survey on smart grid technologies and applications", in *Renewable Energy*, vol. 146, pp. 2589-2625, doi: 10.1016/j.renene.2019.08.092.

[4] NIST (2014), NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0, https://www.nist.gov/el/smart-grid/about-smart-grid/smart-grid-beginners-guide, consultado: agosto 2021.

[5] B. Rokan, and Y. Kotb (2020), "Towards a Real IoT-Based Smart Meter System", in *Advances in Intelligent Systems and Computing*, vol. 1045, doi: 10.1007/978-981-15-0029-9_11.

[6] A. Amara, et al. (2020), "Anomaly-based framework for detecting power overloading cyberattacks in smart grid AMI," in *Computers & Security*, vol. 96, doi: 10.1016/j.cose.2020.101896.

[7] SENER (2017), "Programa de redes eléctricas inteligentes (PRODEREI)", consultado en agosto de 2021, disponible en línea: https://www.gob.mx/cms/upload/attachment/file/250609/2017_Programa_de_Redes_El_ctricas_Inteligentes.pdf

[8] W. Meng, E. W. Tischhauser, Q. Wang, Y. Wang and J. Han (2018), "When Intrusion Detection Meets Blockchain Technology: A Review," in *IEEE Access*, vol. 6, pp. 10179-10188, doi: 10.1109/ACCESS.2018.2799854.

[9] A. Hasankhani, et al. (2021), "Blockchain technology in the future smart grids: A comprehensive review and frameworks," in *International Journal of Electrical Power & Energy Systems*, vol. 129, doi: 10.1016/j.ijepes.2021.106811.

[10] A. A. G. Agung, R. Handayani (2020), "Blockchain for smart grid," in *Journal of King Saud University - Computer and Information Sciences*, doi: 10.1016/j.jksuci.2020.01.002.

[11] Fortune Business Insights (2019), Energía y Renovables. Tamaño del mercado de medidores eléctricos inteligentes, participación y análisis de la industria, 2019-2026.

[12] Comision Federal de Electricidad (2019), "Reporte Anual CFE 2018," Tech. Rep. 1, 2019. Consultado: junio 2021. Disponible en: https://www.cfe.mx/inversionistas/Documents/reporte_anual/Informe%20Anual%20BOLSA%202018.pdf

[13] BearingPoint (2021), "Risk of cyber security attacks on smart grid", consultado en junio de 2021, disponible en: https://www.bearingpoint.com/fr-fr/blogs/energie/risk-of-cyber-security-attacks-on-smart-grid/

[14] Magda Foti, Manolis Vavalis (2021), “What blockchain can do for power grids?,” in *Blockchain: Research and Applications*, vol. 2, no. 1, doi: 10.1016/j.bcra.2021.100008.

[15] A. Agarkar, H. Agrawal (2019), “A review and vision on authentication and privacy preservation schemes in smart grid network,” in *Security and Privacy*, vol. 62, no. 2, doi: 10.1002/spy2.62.

[16] N. Z. Aitzhan and D. Svetinovic (2018), "Security and Privacy in Decentralized Energy Trading Through Multi-Signatures, Blockchain and Anonymous Messaging Streams," in *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 5, pp. 840-852, 1 Sept.-Oct. 2018, doi: 10.1109/TDSC.2016.2616861.

[17] M. Mihaylov, S. Jurado, N. Avellana, K. Van Moffaert, I. M. de Abril and A. Nowé (2014), "NRGcoin: Virtual currency for trading of renewable energy in smart grids," *11th International Conference on the European Energy Market (EEM14)*, 2014, pp. 1-6, doi: 10.1109/EEM.2014.6861213.

[18] Helios (2021), “Helios Protocol”, última consulta: agosto 2021, https://heliosprotocol.io/.

[19] K. Li, et al. (2021), “A lightweight privacy-preserving and sharing scheme with dual-blockchain for intelligent pricing system of smart grid,” in *Computers & Security*, vol. 103, doi: 10.1016/j.cose.2021.102189.

[20] M. Kamal and M. Tariq (2019), "Light-Weight Security and Blockchain Based Provenance for Advanced Metering Infrastructure," in *IEEE Access*, vol. 7, pp. 87345-87356, doi: 10.1109/ACCESS.2019.2925787.

[21] S. -V. Oprea, A. Bâra and A. I. Andreescu (2020), "Two Novel Blockchain-Based Market Settlement Mechanisms Embedded Into Smart Contracts for Securely Trading Renewable Energy," in *IEEE Access*, vol. 8, pp. 212548-212556, doi: 10.1109/ACCESS.2020.3040764.

[22] S. Chen, L. Yang, C. Zhao, V. Varadarajan, K. Wang (2020), “Double-blockchain Assisted Secure and Anonymous Data Aggregation for Fog-enabled Smart Grid,” in *Engineering*, doi: 10.1016/j.eng.2020.06.018.

[23] J. Gao et al. (2018), "GridMonitoring: Secured Sovereign Blockchain Based Monitoring on Smart Grid," in *IEEE Access*, vol. 6, pp. 9917-9925, 2018, doi: 10.1109/ACCESS.2018.2806303.

[24] Y. Sompolinsky, et al. (2018). “PHANTOM: A Scalable BlockDAG protocol” School of Engineering and Computer Science, *The Hebrew University of Jerusalem*, Israel. Última consulta: junio de 2021. Disponible en: https://eprint.iacr.org/2018/104.pdf

[25] M. Cebe, E. Erdin, K. Akkaya, H. Aksu and S. Uluagac (2018), "Block4Forensic: An Integrated Lightweight Blockchain Framework for Forensics Applications of Connected Vehicles," in *IEEE Communications Magazine*, vol. 56, no. 10, pp. 50-57, doi: 10.1109/MCOM.2018.1800137.

[26] P. K. Sharma, M. Chen and J. H. Park (2018), "A Software Defined Fog Node Based Distributed Blockchain Cloud Architecture for IoT," in *IEEE Access*, vol. 6, pp. 115-124, 2018, doi: 10.1109/ACCESS.2017.2757955.

[27] J. Gu, B. Sun, X. Du, J. Wang, Y. Zhuang and Z. Wang (2018), "Consortium Blockchain-Based Malware Detection in Mobile Devices," in *IEEE Access*, vol. 6, pp. 12118-12128, doi: 10.1109/ACCESS.2018.2805783.

[28] M. Fan and X. Zhang (2019), "Consortium Blockchain Based Data Aggregation and Regulation Mechanism for Smart Grid," in *IEEE Access*, vol. 7, pp. 35929-35940, doi: 10.1109/ACCESS.2019.2905298.

[29] Q. Yang and H. Wang, "Privacy-Preserving Transactive Energy Management for IoT-aided Smart Homes via Blockchain," in *IEEE Internet of Things Journal*, doi: 10.1109/JIOT.2021.3051323.

[30] M. Afzal, Q. Huang, W. Amin, K. Umer, A. Raza and M. Naeem (2020), "Blockchain Enabled Distributed Demand Side Management in Community Energy System With Smart Homes," in *IEEE Access*, vol. 8, pp. 37428-37439, doi: 10.1109/ACCESS.2020.2975233.

[31] S. Zhang, J. Rong, B. Wang (2020), "A privacy protection scheme of smart meter for decentralized smart home environment based on consortium blockchain," in *International Journal of Electrical Power & Energy Systems*, vol. 121, doi: 10.1016/j.ijepes.2020.106140.

[32] GridPlus (2021), https://gridplus.io/ Última consulta: agosto de 2021.

[33] PowerLedger (2021), https://powerledger.io/ Última consulta: agosto de 2021.

[34] LO3 Energy (2021), https://lo3energy.com/ Última consulta: agosto de 2021.

[35] Jiangsu Rongze Information Technology (2020), "Power system electricity consumption usage data statistics management system based on block chain", Patente CN111475581 A, https://patents.google.com/patent/CN111475581A/en?oq=CN111475581+A

[36] North China Electric Power University (2019), "Distributed generation energy management method based on block chain double-chain structure", Patente CN111062596 A, https://patents.google.com/patent/CN111062596A/en?oq=CN111062596+A

[37] China Southern Power Grid Co Ltd Institute of Information Engineering of CAS (2019), "Block chain-based electricity consumption client credit management method and system", Patente CN110704531 A, https://patents.google.com/patent/CN110704531A/en?oq=CN110704531+A

[38] Chung Ang University Industry Academic Cooperation Foundation (2018), "Blockchain-based secure smart grid management system", Patente KR20200063623 A, https://patents.google.com/patent/KR20200063623A/en?oq=KR20200063623+A

[39] Timothy MAYNE, Serge UMANSKY (2017), "Method of matching renewable energy production to end-user consumption via blockchain systems", Patente

US20190164236 A1, https://patents.google.com/patent/US20190164236A1/en?oq=US20190164236+A1

[40] International Business Machines Corp (2018), "Method or system for management of a device for energy consumption by applying blockchain protocol", Patente US20190353685 A1, https://patents.google.com/patent/US20190353685A1/en?oq=US20190353685+A1

[41] Accenture Global Solutions Ltd (2016), "Device, method and system for autonomous selection of a commodity supplier through a blockchain distributed database", Patente US20170206522 A1, https://patents.google.com/patent/US20170206522A1/en?oq=US20170206522+A1

[42] Juan C. Olivares-Rojas, Enrique Reyes-Archundia, José A. Gutiérrez-Gnecchi, Jaime Cerda-Jacobo, and Johan W. González-Murueta (2020), "A Novel Multi-Tier Blockchain Architecture to Protect Data in Smart Metering Systems", in *IEEE Transactions on Engineering Management*, Special Issue on Blockchain Ecosystems, vol. 67, no. 4, doi: 10.1109/TEM.2019.2950410.

[43] Juan C. Olivares-Rojas, Enrique Reyes-Archundia, Jose A. Gutiérrez-Gnecchi, Johan W. González-Murueta, Jaime Cerda-Jacobo (2020), "A multi-tier architecture for data analytics in smart metering systems", in *Simulation Modelling Practice and Theory*, special issue on IoT, Cloud, Big Data and AI in Interdisciplinary Domains , Elsevier, Vol. 102, doi: 10.1016/j.simpat.2019.102024.

[44] Juan C. Olivares-Rojas, Enrique Reyes Archundia, José A. Gutiérrez-Gnechi, Ismael Molina-Moreno, Jaime Cerda-Jacobo, Arturo Méndez-Patiño (2021), "A Transactive Energy Model for Smart Metering Systems using Blockchain", in *CSEE Journal of Power & Energy Systems*, doi: 10.17775/CSEEJPES.2020.05670.

[45] Juan C. Olivares-Rojas, Enrique Reyes Archundia, José A. Gutiérrez-Gnechi, Ismael Molina-Moreno, Jaime Cerda-Jacobo, Arturo Méndez-Patiño (2021), "Towards Cybersecurity of the Smart Grid using Digital Twins", in *IEEE Internet Computing*, doi: 10.1109/MIC.2021.3063674.

[46] Juan C. Olivares-Rojas, Enrique Reyes-Archundia, José A. Gutiérrez-Gnecchi, Jorge L. Diaz-Huerta, Jaime Cerda-Jacobo, Adriana C. Téllez-Anguiano, Johan W. González-Murueta (2020), "Data Analytics of Electromagnetics Field Measurements in Smart Meters", in *International Journal of Combinatorial Optimization Problems and Informatics*, Vol. 11, No. 2, https://ijcopi.org/ojs/article/view/165.

[47] Juan C. Olivares-Rojas, Enrique Reyes Archundia, José A. Gutiérrez-Gnechi, Ismael Molina-Moreno, Jaime Cerda-Jacobo, Arturo Méndez-Patiño (2021), "A Methodology for Cyber Hygiene in Smart Grids", in *Revista Dyna Ingeniería e Industria*, https://www.revistadyna.com/ (por aparecer).

[48] P. V. Aubel, E. Poll (2019), "Smart metering in the Netherlands: What, how, and why," in *International Journal of Electrical Power & Energy Systems*, vol. 109, 2019, pp. 719-725, doi: 10.1016/j.ijepes.2019.01.001.

[49] New Energy News (2021), http://newenergynews.blogspot.com/, Última consulta: agosto 2021.

[50] WebNMS (2021), "IoT Division of Zoho Corporation", http://webnms.com, Última consulta: agosto 2021.

[51] O. Abrishambaf, et al. (2019), "Towards transactive energy systems: An analysis on current trends," in *Energy Strategy Reviews*, vol. 26, doi: 10.1016/j.esr.2019.100418.

[52] Q. Sun et al. (2016), "A comprehensive review of smart energy meters in intelligent energy networks," in *IEEE Internet Things Journal*, vol. 3, no. 4, pp. 464–479, doi: 10.1109/JIOT.2015.2512325.

[53] Y. Wang, Q. Chen, T. Hong, and C. Kang (2019), "Review of Smart Meter Data Analytics: Applications, Methodologies, and Challenges," in *IEEE Transactions on Smart Grid*, vol. 10, no. 3, pp. 3125–3148, doi: 10.1109/TSG.2018.2818167.

[54] J. D. Hmielowski, A. D. Boyd, G. Harvey, J. Joo (2019), "The social dimensions of smart meters in the United States: Demographics, privacy, and technology readiness," in *Energy Research & Social Science*, vol. 55, pp. 189-197, doi: 10.1016/j.erss.2019.05.003.

[55] A. R. Singh, D. Devaraj, R. N. Banu (2019), "Genetic algorithm-based optimisation of load-balanced routing for AMI with wireless mesh networks," in *Applied Soft Computing*, vol. 74, pp. 122-132, doi: 10.1016/j.asoc.2018.10.003

[56] D. B. Avancini, J.P.C. Rodrigues, S. G.B. Martins, R. A.L. Rabêlo, J. Al-Muhtadi, P. Solic (2017), "Energy meters evolution in smart grids: A review," in *Journal of Cleaner Production*, vol. 217, pp. 702-715, doi: 10.1016/j.jclepro.2019.01.229.

[57] I. Bayram, and T. Ustun (2017), "A survey on behind the meter energy management systems in smart grid," in *Renewable and Sustainable Energy Reviews*, vol. 72, pp. 1208-1232, doi: 10.1016/j.rser.2016.10.034.

[58] C. Miyachi (2018), "What is "Cloud"? It is time to update the NIST definition?," in *IEEE Cloud Computing*, vol. 5, no. 3, pp. 6-11, doi: 10.1109/MCC.2018.032591611.

[59] B. W. Nyamtiga, J. C. S. Sicato, S. Rathore, Y. Sung and Jong Hyuk Park (2019), "Blockchain-Based Secure Storage Management with Edge Computing for IoT," in *Electronics*, vol. 8, no. 828, doi:10.3390/electronics8080828.

[60] WinSystems (2021) "Cloud fog and edge computing—What's the difference?", https://www.winsystems.com/cloud-fog-and-edge-computing-whats-the-difference/, Última consulta: agosto 2021.

[61] A. Rivaldo (2012), "Health and RF EMF from Advanced Meters an Overview of Recent Investigations and Analyses" in *Public Utility Commission of Texas Infrastructure & Reliability Division*, http://www.puc.texas.gov/industry/electric/reports/smartmeter/smartmeter_rf_emf_health_12-14-2012.pdf, Última consulta: agosto 2021.

[62] L. Burel (2021), "How To Understand The Different Measurement Units That Are Used To Measure EMFs", https://www.electricsense.com/3772/how-to-understand-the-different-measurement-units-that-are-used-to-measure-emfs, Última consulta: agosto 2021.

[63] California Council on Science and Technology (2011), "Health impacts of radio frequency exposure from smart meters", ISBN-13: 978-1-930117-42-6, https://ccst.us/wp-content/uploads/2011smart-final.pdf, Última consulta: agosto 2021.

[64] R. Tell (2021), "Supplemental Report on An Analysis of Radiofrequency Fields Associated with Operation of the PG&E Smart Meter Program Upgrade System", Richard Tell Associates, http://www.pge.com/includes/docs/pdfs/shared/edusafety/systemworks/rfsafety/rf_fields_supplemental_report_2008.pdf, Última consulta: agosto 2021.

[65] Electric Power Research Institute (2011), "Radio-Frequency Exposure Levels from Smart Meters: A Case Study of One Model", https://www.smartgrid.gov/files/RadioFrequency_Exposure_Levels_from_Smart_Meters_Case_Study_201106.pdf, Última consulta: agosto 2021.

[66] ICS-CERT (2021), "Industrial Control Systems -", https://us-cert.cisa.gov/ics, Última consulta: agosto de 2021.

[67] J. Laufs, et al. (2020), "Security and the smart city: A systematic review," in *Sustainable Cities and Society*, vol. 55, doi: 10.1016/j.scs.2020.102023.

[68] R. Ande, et al. (2020). "Internet of Things: Evolution and technologies from a security perspective," in *Sustainable Cities and Society*, vol. 54, doi: 10.1016/j.scs.2019.101728.

[69] H. Habibzadeh, et al. (2019), "A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities," in *Sustainable Cities and Society*, vol. 50, doi: https://doi.org/10.1016/j.scs.2019.101660.

[70] M. Zekeriya, and R. Das (2020), "Cyber-security on smart grid: Threats and potential solutions," in *Computer Networks*, vol. 169, doi: 10.1016/j.comnet.2019.107094.

[71] P. Kumar, Y. Lin, G. Bai, A. Paverd, J. S. Dong and A. Martin (2019), "Smart Grid Metering Networks: A Survey on Security, Privacy and Open Research Issues," in *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2886-2927, doi: 10.1109/COMST.2019.2899354.

[72] J. Giraldo, A. Cárdenas and N. Quijano (2017), "Integrity Attacks on Real-Time Pricing in Smart Grids: Impact and Countermeasures," in *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2249-2257, doi: 10.1109/TSG.2016.2521339.

[73] Y. He, G. J. Mendis and J. Wei, "Real-Time Detection of False Data Injection Attacks in Smart Grid: A Deep Learning-Based Intelligent Mechanism," in *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2505-2516, doi: 10.1109/TSG.2017.2703842.

[74] R. Deng, G. Xiao, R. Lu, H. Liang and A. V. Vasilakos (2017), "False Data Injection on State Estimation in Power Systems—Attacks, Impacts, and Defense: A Survey," in *IEEE Transactions on Industrial Informatics*, vol. 13, no. 2, pp. 411-423, doi: 10.1109/TII.2016.2614396.

[75] T. Liu, J. Tian, Y. Gui, Y. Liu and P. Liu (2017), "SEDEA: State Estimation-Based Dynamic Encryption and Authentication in Smart Grid," in *IEEE Access*, vol. 5, pp. 15682-15693, doi: 10.1109/ACCESS.2017.2713440.

[76] D. Abbasinezhad-Mood and M. Nikooghadam (2018), "An Ultra-Lightweight and Secure Scheme for Communications of Smart Meters and Neighborhood Gateways by Utilization of an ARM Cortex-M Microcontroller," in *IEEE Transactions on Smart Grid*, doi: 10.1109/TSG.2017.2705763.

[77] M. M. E. A. Mahmoud, N. Saputro, P. K. Akula and K. Akkaya (2017), "Privacy-Preserving Power Injection Over a Hybrid AMI/LTE Smart Grid Network," in *IEEE Internet of Things Journal*, vol. 4, no. 4, pp. 870-880, doi: 10.1109/JIOT.2016.2593453.

[78] M. M. N., and W. H. Hassan (2019), "Current research on Internet of Things (IoT) security: A survey", in *Computer Networks*, vol. 148, pp. 283-294, doi: 10.1016/j.comnet.2018.11.025.

[79] A. Vishwanath, et al. (2020). "Cyber hygiene: The concept, its measure, and its initial tests," in *Decision Support Systems*, vol. 128, doi: 10.1016/j.dss.2019.113160.

[80] R. Clint (2019), "DLT/Blockchain as a Building Block for Enterprise Transformation," in *IEEE Engineering Management Review*, doi: 10.1109/EMR.2019.2895303.

[81] A. S. Musleh, G. Yao and S. M. Muyeen (2019), "Blockchain Applications in Smart Grid–Review and Frameworks," in *IEEE Access*, vol. 7, pp. 86746-86757, doi: 10.1109/ACCESS.2019.2920682.

[82] T. M. Fernández-Caramés and P. Fraga-Lamas (2018), "A Review on the Use of Blockchain for the Internet of Things," in *IEEE Access*, vol. 6, pp. 32979-33001, doi: 10.1109/ACCESS.2018.2842685.

[83] A. Aderibole et al. (2020), "Blockchain Technology for Smart Grids: Decentralized NIST Conceptual Model," in *IEEE Access*, vol. 8, pp. 43177-43190, doi: 10.1109/ACCESS.2020.2977149.

[84] P. Zhuang, T. Zamir and H. Liang (2021), "Blockchain for Cybersecurity in Smart Grid: A Comprehensive Survey," in *IEEE Transactions on Industrial Informatics*, vol. 17, no. 1, doi: 10.1109/TII.2020.2998479.

[85] M. A. Ferrag and L. Maglaras (2020), "DeepCoin: A Novel Deep Learning and Blockchain-Based Energy Exchange Framework for Smart Grids," in *IEEE Transactions on Engineering Management*, vol. 67, no. 4, pp. 1285-1297, doi: 10.1109/TEM.2019.2922936.

[86] Y. Yuan and F. Wang (2018), "Blockchain and Cryptocurrencies: Model, Techniques, and Applications," in *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 48, no. 9, pp. 1421-1428, doi: 10.1109/TSMC.2018.2854904.

[87] S. M. A. A. Abir, A. Anwar, J. Choi and A. S. M. Kayes (2021), "IoT-Enabled Smart Energy Grid: Applications and Challenges," in *IEEE Access*, vol. 9, pp. 50961-50981, 2021, doi: 10.1109/ACCESS.2021.3067331.

[88] A. Pinna, S. Ibba, G. Baralla, R. Tonelli and M. Marchesi (2019), "A Massive Analysis of Ethereum Smart Contracts Empirical Study and Code Metrics," in *IEEE Access*, vol. 7, pp. 78194-78213, doi: 10.1109/ACCESS.2019.2921936.

[89] T. Alladi, et al. (2020), "Blockchain in Smart Grids: A Review on Different Use Cases," in *Sensors*, vol. 19, doi: 10.3390/s19224862.

[90] K. Alabi (2017), "Digital blockchain networks appear to be following Metcalfe's Law," in *Electronic Commerce Research and Applications*, vol. 24, pp. 23-29, doi: 1567-4223.

[91] S. Sayeed, H. Marco-Gisbert (2019), "Assessing Blockchain Consensus and Security Mechanisms against the 51% Attack", in *Applied Sciences*, vol. 9, no. 1788, doi: 10.3390/app9091788.

[92] S. Eisele, et al. (2020), "Blockchains for Transactive Energy Systems: Opportunities, Challenges, and Approaches," in *Computer*, vol. 53, no. 9, pp. 66-76, doi: 10.1109/MC.2020.3002997.

[93] Indigo Advisory (2019), "Blockchain in Energy and Utilities", Disponible en: https://www.indigoadvisorygroup.com/blockchain/, última consulta: agosto 2021.

[94] C. Liu, X. Zhang, K. K. Chai, J. Loo, and Y. Chen (2021), "A survey on blockchain-enabled smart grids: Advances, applications and challenges," in *IET Smart Cities*, vol. 3, pp. 56-78, doi: 10.1049/smc2.12010.

[95] M. Mollah, et al. (2021), "Blockchain for Future Smart Grid: A Comprehensive Survey," in *IEEE Internet of Things Journal*, vol. 8, no. 1, pp. 18-43, doi: 10.1109/JIOT.2020.2993601.

[96] A. Faruqui and C. Bourbonnais (2020), "The Tariffs of Tomorrow: Innovations in Rate Designs," in *IEEE Power and Energy Magazine*, vol. 18, no. 3, pp. 18-25, doi: 10.1109/MPE.2020.2972136.

[97] A. Diaz and C. van Beers (2013), "Energy subsidies, structure of electricity prices and technological change of energy use," in *Energy Economics*, vol. 40, pp. 495-502, doi: 10.1016/j.eneco.2013.08.002.

[98] R. Moreno et al. (2020), "Distribution Network Rate Making in Latin America: An Evolving Landscape," in *IEEE Power and Energy Magazine*, vol. 18, no. 3, pp. 33-48, 2020, doi: 10.1109/MPE.2020.2972667.

[99] C. Puckett et al. (2020), "Utility Load Research: The Future of Load Research Is Now," in *IEEE Power and Energy Magazine*, vol. 18, no. 3, pp. 61-70, doi: 10.1109/MPE.2020.2972668.

[100] Comisión Federal de Electricidad (2021), "Mexican Electricity Rates", https://www.cfe.mx/tarifas/Pages/Tarifas.aspx, Última consulta: agosto 2021.

[101] Y. Sook-Chin, et al. (2018), "An anomaly detection framework for identifying energy theft and defective meters in smart grids," in *International Journal of Electrical Power & Energy Systems*, vol. 101, pp. 189-203, doi: 10.1016/j.ijepes.2018.03.025.

[102] Y. Sook-Chin, et al. (2017), "Detection of energy theft and defective smart meters in smart grids using linear regression," in *International Journal of Electrical Power & Energy Systems*, vol. 91, pp. 230-240, doi: 10.1016/j.ijepes.2017.04.005.

[103] A. M. Karimi-Majd, M. Mahootchi, A. Zakery (2017), "A reinforcement learning methodology for a human resource planning problem considering knowledge-based promotion" in *Simulation Modelling Practice and Theory*, vol. 79, pp. 87-99, doi: 10.1016/j.simpat.2015.07.004.

[104] W. Zhu, W. Yu, B. Kan and G. Liu (2017), "Smart Meter Data Analytics Based on Modified Streaming k-Means," *2017 3rd International Conference on Big Data Computing and Communications (BIGCOM)*, pp. 328-333. doi: 10.1109/BIGCOM.2017.49.

[105] D. Saxena, K.S. Verma, and S.N. Singh (2010), "Power quality event classification: an overview and key issues" in *International Journal of Engineering, Science and Technology*, vol. 2, no. 3, pp. 186-199, https://pdfs.semanticscholar.org/a4fb/cb3166e9f8c7e126d993df5d101018ef630c.pdf, Última consulta: agosto 2021.

[106] nD-enerserve GmbH (2019), "SmartPi", https://blog.enerserve.eu/category/smartpi/installation-smartpi/, Última consulta: agosto 2021.

[107] Fuller, A., et al. (2020), "Digital Twin: Enabling Technologies, Challenges and Open Research," in *IEEE Access*, vol. 8, pp. 108952-108971, DOI: 10.1109/ACCESS.2020.2998358.